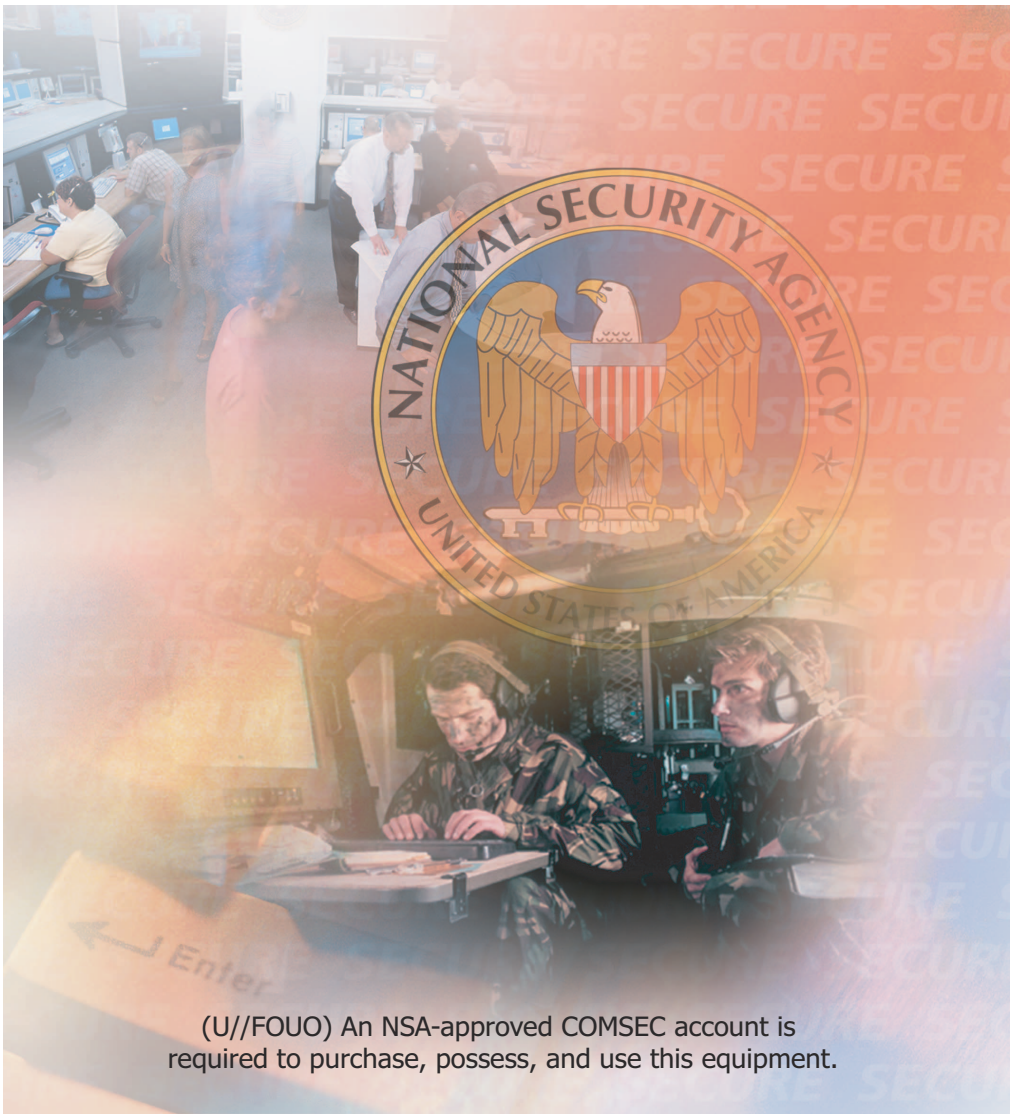
SecNet 54®

Secure Network Products



(U//FOUO) USER MANUAL FOR THE KIV-54RM01

P/N 12071-7012A
xx xxxxxx 2010

WARNING

(U) This document contains information controlled by the International Traffic in Arms Regulations (22 CFR 120-130) of the United States of America. The resale, diversion, transfer, or disposal of this document or any other element of the SecNet 54® software is restricted by the END USER License Agreement for the SecNet 54® software.

HARRIS®

assuredcommunications®

Harris Corporation - Export Controlled Document

(U) Copyright

(U) HARRIS CORPORATION

P/N 12071-7012

(U) Harris Corporation - RF Communications Division

1680 University Avenue

Rochester, NY 14610

USA Phone Numbers: 585-244-5830 | 585-242-4319 | 1-866-264-8040 toll-free

USA Fax Phone Numbers: 585-242-4755 | 585-242-4490

Revision Status

UNCLASSIFIED

Revision	Change Details	Issue Date
-	Re-issue manual to reflect 2.0 Baseline and new document part number. Refer to part number 7017340 for earlier versions of this manual. ECO C42352	17 October 2008
A	Updated document with Unclassified//For Official Use Only (FOUO) classification markings. Build 2.1 Release. ECO xxxx	

UNCLASSIFIED

(U) Table of Contents

(U) Table of Contents

(U) Table of Contents

(U) Table of Contents

(U) Table of Contents

(U) Table of Contents

Paragraph **Title** **Page**

This page intentionally left blank.

(U) Safety Information

(U) Before setting up and operating the SecNet 54® devices, please refer to important safety guidelines and instructions in Chapter 2 of this manual.

(U) Introduction

(U) This manual is organized into several chapters, providing general information on the SecNet 54® devices (KIV-54, RM01, etc.), and detailing specific information for the User on setup, assembly, and device monitoring and configuration. Some duplication of material may occur throughout. The following list describes the content of each chapter.

- (U) Chapter 1, Introduction, provides an overview of the SecNet 54® products and the requirements for using them.
- (U) Chapter 2, Hardware Setup, provides information on assembling the SecNet 54® modules and attaching them to a network.
- (U) Chapter 3, Device Configuration and Monitoring, describes the method for locating SecNet 54® products on the network, configuring them and monitoring their status.
- (U) Chapter 4, KIV-54RM01 Operations, describes procedures for setting up and configuring the KIV-54RM01; for operating the device to provide client communications; and for rebooting and zeroizing the device.
- (U) Appendices provide the following additional information:
  - (U) Appendix A, Acronyms, Abbreviations, and Glossary, defines acronyms and terms.
  - (U) Appendix B, Frequently Asked Questions (FAQ)s, answers common questions about the cryptographic and external models' functionality.
  - (U) Appendix C, Technical Support and Contact Information, describes the SecNet 54® support policy.
  - (U) Appendix D, Warranty, describes SecNet 54® product family warranty information.
  - (U) Appendix E, Specifications, lists SecNet 54® equipment specifications.
  - (U) Appendix F, Factory Default Settings, lists factory default settings for the SecNet 54® products.
  - (U) Appendix G, Importing SecNet 54 Secure Socket Layer (SSL) Certificates into Web Browsers, describes the import process (i.e., installation) associated with three common Web browsers.
  - (U) Index, provides a quick reference to information contained in this manual.

(U) SecNet 54 ® User Manual for the KIV-54RM01

(U) About this Manual

NOTE

(U) Windows displayed in this manual are sample representations of the SecNet 54® software applications and Web pages. Data displayed within the windows in real time may differ from this manual due to the SecNet 54® device being used, software and firmware revisions, and the Web browser selected to access the configuration Web pages.

(U) Documentation Conventions

(U) The following documentation conventions are used in this manual for notes, special symbols, and emphasized text.

NOTE

(U) The **NOTE** is used to provide additional information or emphasis to the User.

(U) The **CAUTION** symbol is used when an operation, procedure or condition, if not strictly observed, would result in equipment damage.

(U) The **WARNING** symbol is used to indicate a potentially hazardous situation which, if not avoided, could result in serious injury to personnel.

(U) Boldface Text

- (U) Window titles
- (U) Status page titles on configuration Web pages
- (U) Option buttons
- (U) Web browser menu options
- (U) Emphasis on specific User prompts and other specific text

(U) Boldface, Blue Text

- (U) Path names

(U) Italic Text

- (U) System messages displayed in generic browser pop-up windows

(U) Underlined Text

- (U) Hyperlinks on configuration Web pages

(U) Courier New Font Text

- (U) Text displayed in the computer's command line

Chapter 1

(U) INTRODUCTION

1.1 (U) CHAPTER CONTENTS

(U) This chapter contains the following information:

- (U) A description of SecNet 54®
- (U) A description of the modular concept
- (U) A description of each module
- (U) The contents of each SecNet product package
- (U) The Hardware (HW) and Software (SW) system requirements for operating this product

1.2 (U) SECNET 54® DESCRIPTION

(U//FOUO) SecNet 54® is a line of secure network products providing National Security Agency (NSA) Type-1, IP encryption. The products are designed for applications requiring up to Top Secret communications. Using the Harris Sierra II Cryptographic processor, which is NSA certified for Top Secret voice and data traffic, these products support High Assurance Internet Protocol Interoperability Specification (HAIPIS) formatted packets.

(U//FOUO) SecNet 54® products are small enough to be held in the hand and weigh less than one pound. Flexibility is designed in, starting with a modular architecture that allows the User (or Administrator) to send secure data over various protocols (802.3 and 802.11 are currently available). The products can be powered by external AC or DC power supplies and are also compatible with Power over Ethernet (PoE). Both electrical and optical 802.3 Ethernet connections are provided for connecting SecNet 54® products to a classified network. Configuration and monitoring are accomplished using platform independent Java applications and secure browser connections.

(U//FOUO) SecNet 54® products are configured and managed by logging into the device using an authorized account. Each SecNet 54® login account is assigned one of two privilege levels when the account is added to the device. These privilege levels are designated as Administrator and User.

(U) A User has the following privileges:

- (U//FOUO) Use a pre-configured device for secure network communications
- (U//FOUO) Monitor the device being used
- (U//FOUO) View the current status of the device
- (U//FOUO) Modify basic Black-side communication parameters
- (U//FOUO) Change personal account password
- (U//FOUO) View the Red and Black network configurations
- (U//FOUO) View device Security Classification Level
- (U//FOUO) View Traffic Flow Security (TFS) settings
- (U//FOUO) Load and view customer-developed Red Security certificates (SSL Certification Authority (CA) and Public/Private Key Pairs) and Black certificates (Wi-Fi Protected Access 2 (WPA2) Enterprise and VPN authentication)
- (U//FOUO) View loaded Pre-placed Keys (PPKs), PPK Chains, FIREFLY Vectors, and P^3 dePAC Moduli
- (U//FOUO) View High Assurance Internet Protocol Encryptor (HAIPE) tunnels

- (U//FOUO) View Dynamic Discovery Communities of Interest (COI) configurations
- (U//FOUO) View Red-side Routing/Routing Information Protocol version 2 (RIPv2) configuration and Routing Table
- (U//FOUO) View and download the audit log
- (U//FOUO) Reboot the device
- (U//FOUO) Zeroize the device

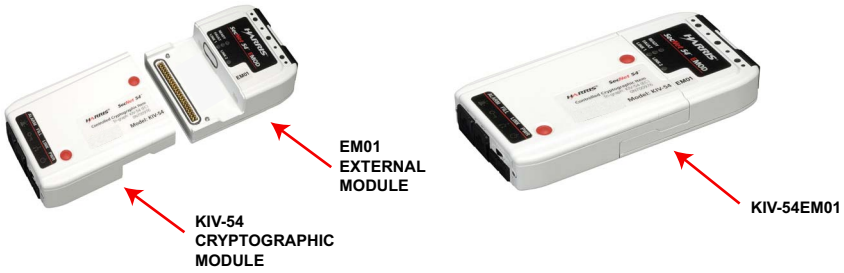
1.2.1 (U) Modular Concept

(U//FOUO) The SecNet 54® device consists of modular hardware that provides secure encrypted network communication. Two modules are connected together to form a functioning device. A Cryptographic Module (CMOD) performs data encryption and decryption, while an attached External Module (XMOD) provides the Black side media interface. This modular approach is cost effective, flexible and expandable. A single CMOD can be paired with any of several XMODs to create a secure encrypted network device for use on a specific transmission medium.

(U//FOUO) The SecNet 54® CMOD is also referred to in this manual by its model number, KIV-54. The first available XMOD is an 802.11 wireless radio, which is also referred to by its model number, RM01. When the RM01 XMOD is attached to the KIV-54 CMOD, the combined SecNet 54® device is referred to as KIV-54RM01. Also available is the 802.3 Ethernet module. The 802.3 Ethernet module is also referred to by its model number, EM01. When the EM01 is attached to the KIV-54 EM0D, it is referred to as KIV-54EM01.

(U) The terms Cryptographic Module (or CMOD) and External Module (or XMOD) are used in this manual when referring generically to these module types.

UNCLASSIFIED//FOUO



UNCLASSIFIED//FOUO

NOTE

(U) For additional information about the 802.3 Ethernet module (EM01), refer to the latest version of the SecNet 54® User manual for the KIV-54EM01 (P/N 12071-7014).

1.2.1.1 (U) KIV-54 Cryptographic Module

(U//FOUO) The KIV-54 has the capability to provide NSA Type-1 encryption, and it is compatible with the key requirements of the High Assurance Internet Protocol Interoperability Specification (HAIPIS) version 1.3.5. The KIV-54 Module is a Controlled Cryptographic Item (CCI) prior to activating a key. The KIV-54's security classification is set by the Administrator through the configuration Web pages, and the KIV-54 only accepts or establishes active keys compatible to its classification level.

(U) KIV-54 operates from Direct Current (DC) power input that is supplied by an AC power supply, external battery, or a wired Ethernet connection with PoE capability. The KIV-54 supplies power to the external module.

1.2.1.2 (U) RM01 External Radio Module

(U//FOUO) The RM01 operates using standard IEEE 802.11 a, b, or g wireless local area network (WLAN) protocol, which supports the following frequencies and data rates:

(U) **Frequency Bands:**

(U) 5GHz (802.11a mode)

(U) 2.4GHz (802.11b/g modes)

(U) **Data Rates:**

(U) 802.11a: 6, 9, 12, 18, 24, 36, 48, 54 Mbps

(U) 802.11b: 1, 2, 5.5,11 Mbps

(U) 802.11g: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps

(U) Two SMA-style screw-on antennas come standard with the RM01 and provide omni-directional coverage. These antennas swivel and tilt to allow the relative position of the transmit and receive antenna to be adjusted.

(U//FOUO) The RM01 can be configured as an Access point (AP), Infrastructure or Ad Hoc Station (STA), or a Wireless Bridge (WB).

1.3 (U) PACKAGE CONTENTS

(U) This section describes the package contents for each of the SecNet 54® products. Refer to the appropriate subsection for each package.

1.3.1 (U) KIV-54 Package Contents

a. (U//FOUO) KIV-54 Module (1)

b. (U) Universal Power Adapter (1)

c. (U) Ethernet Cable (1)

d. (U//FOUO) SecNet 54® Manuals CD (1), containing the following:

- (U) Autorun file
- (U) Getting Started file

- (U//FOUO) SecNet 54® Administrator Manuals (2)
- (U//FOUO) SecNet 54® User Manuals (2)
- (U) End User License Agreement (EULA)
- (U) Installation Instructions (Java, SSL Policy files, and Acrobat Reader)
- (U) Java Runtime Environment (JRE) JAR files (2)
- (U) Adobe Acrobat Reader

e. (U//FOUO) SecNet 54® Applications CD (1), containing the following:

- (U) Autorun file
- (U//FOUO) Device Management Utility (DMU) Software
- (U//FOUO) SecNet 54® SSL CA Certificate
- (U//FOUO) SecNet 54® SSL Client Certificate
- (U) Java Runtime Environment (JRE) Software
- (U) Java Crypto Policy Files (.Jar) (2)
- (U) Adobe Acrobat Reader
- (U) EULA
- (U) Installation Instructions (Java, SSL Policy files, and Acrobat Reader)

1.3.2 (U) RM01 Package Contents

- (U//FOUO) RM01 Module (1)
- (U) RM01 Antennas (2)
- (U) Antenna Terminator (1)

1.4 (U) SYSTEM REQUIREMENTS

1.4.1 (U) Hardware

(U//FOUO) The KIV-54 can support two sources of external power, an external power supply and a battery. The KIV-54 universal power supply uses standard wall power 100 - 240 VAC at 47 - 63 Hz. The operating DC input is 14V - 30V. Additionally, the KIV-54 adheres to standard PoE Power Constraints.

CAUTION (U) The KIV-54 case may become hot to the touch in high ambient temperature environments.

1.4.2 (U) Software

(U//FOUO) The SecNet 54® software applications require the installation of JRE Java 2 Standard Edition (J2SE) version 1.4.2. The JRE for several operating systems is provided on the SecNet 54® Applications CD shipped with the KIV-54. Additionally, multiple versions of the JRE can be found on the SUN website.

(U//FOUO) A Web browser is required for using the KIV-54 configuration Web pages. This browser must meet the following constraints to support the Web pages.

- (U) Enabled Java Script
- (U) Enabled Cookies
- (U) Support of CSS 2.1 and HTML 4.01
- (U) Support of SSL/Transport Layer Security (TLS)

(U//FOUO) Note that KIV-54 will negotiate up to AES 256 bit encryption and will work with browsers that use lower level encryption.

Chapter 2

(U) HARDWARE SETUP

2.1 (U) CHAPTER CONTENTS

(U) This chapter contains the following information:

- (U) Critical safety information for setting up and operating the KIV-54 cryptographic module with external modules
- (U) Illustrations and descriptions of the KIV-54 cryptographic module and an external module
- (U) Details on attaching an external module to the KIV-54 cryptographic module
- (U) Details on applying power to the KIV-54 cryptographic module
- (U) Details on connecting the KIV-54 cryptographic module to the network
- (U) Details on using the KIV-54RM01 outdoors

2.2 (U) SAFETY INFORMATION

(U) Read the following safety information to understand the proper use of equipment and to prevent harm to personnel and/or damage to the modules.

2.2.1 (U) KIV-54 Cryptographic Module Safety Information

CAUTION

(U) Ensure that the power switch of the KIV-54 Cryptographic Module is in the Off position before attaching or detaching external modules.

2.2.2 (U) RM01 Radio Module Safety Information

(U) Operate the RM01 Radio Module in accordance with the instructions found in this manual to minimize exposure to Radio Frequency (RF) energy. Even though the RM01 does not fall under Federal Communications Commission (FCC) regulations for government use, it should be operated in conformance with generally accepted safety standards for human exposure to RF electromagnetic energy as emitted by similar FCC-certified equipment.

(U) The use of external amplifiers and/or antennas not supplied with the basic RM01 configuration would likely put the equipment into a different equipment category. That is, the equipment would then require additional installation procedures, warning instructions and/or warning labels as mandated by the third party RF equipment provider. It would also require that professional installers and end-users be supplied with antenna pointing instructions and warnings to others to maintain specified distances from the antenna(s).

2.2.2.1 (U) RM01 General Precautions

(U) The FCC is required by the National Environmental Policy Act of 1969 to evaluate the effect of emissions from FCC-regulated transmitters on the quality of the human environment. At the present time there is no federally mandated RF exposure standard. However, several non-government organizations, such as the American National Standards Institute (ANSI), the Institute of Electrical and Electronics Engineers, Inc. (IEEE), and the National Council on Radiation Protection and Measurements (NCRP) have issued recommendations for human exposure to RF electromagnetic fields. The potential hazards

associated with RF electromagnetic fields are discussed in the Office of Engineering and Technology (OET) Bulletin No. 56, "Questions and Answers about the Biological Effects and Potential Hazards of Radio frequency Electromagnetic Fields." Further information on evaluating compliance with limits can be found in the FCC's OET Bulletin Number 65, "Evaluating Compliance with FCC Guidelines for Human Exposure to Radio frequency Electromagnetic Fields."

(U) The FCC has set a general guideline of 20 cm (8 inches) separation between the device and the body, for use of a wireless device near the body (this does not include extremities). Therefore, the user shall observe the FCC RF Exposure limits distance separation of 20 cm in controlled and uncontrolled configurations. Furthermore, this device shall be used in such a manner that the potential for human contact during normal operation is minimized.

NOTE

(U) The Maximum Permissible Exposure (MPE) calculation is based on FCC Part 1.1310 Table 1 limits, which state that the power density for uncontrolled exposure is 1mW/cm^2 for systems operating in the ISM and UNII band.

(U) Proper operation of this radio device according to the instructions in this publication will result in user exposure below the FCC recommended limits.

WARNING

(U) To maintain conformity with RF exposure guidelines, this equipment should be installed and operated with proper distance between the radiator and the body while using the supplied antennas. Unauthorized antennas, modification, or attachments could damage the transmitter and may violate FCC regulations.

2-2.2.1.1 (U) RM01 Safety Guidelines

(U) Follow the safety guidelines set forth in this paragraph when operating the RM01.

- (U) Minimize contact time when moving the antenna while the unit is transmitting or receiving.
- (U) Do not orient antennas such that they are in contact with the skin.
- (U) Do not orient antennas such that they are in contact with a metal surface.
- (U) Do not hold any component containing a radio such that the antenna is very close to or touching any exposed parts of the body, especially the face or eyes, while transmitting.

CAUTION

(U) Do not operate the RM01 or attempt to transmit data unless the antennas are connected. Operating the RM01 without antennas can damage the unit. Always terminate unused antenna ports with a 50 Ohm SMA terminator.

(U) Do not let the antennas touch each other during operation. Do not over-torque the SMA antennas or any other connectors to the RM01 SMA connectors. Connector torque specification should not exceed 8 inch - pounds.

2-2.2.1.2 (U) RM01 Safety Guidelines for Use in a Specific Environment

(U) When in certain environments, specific additional safety guidelines apply. Follow the guidelines listed below when in these types of environments.

- (U) The use of wireless devices in hazardous locations is limited to the constraints posed by the safety directors of such environments.
- (U) The use of wireless devices on airplanes is governed by the Federal Aviation Administration (FAA).
- (U) The use of wireless devices in hospitals is restricted to the limits set forth by each hospital.

⚠WARNING

(U) Do not operate the wireless network device near unshielded blasting caps or in an explosive environment unless the device has been modified to be especially qualified for such use.

(U) Use in other configurations may not ensure conformity with FCC RF exposure guidelines.

2.2.2.2 (U) Antennas - SMA Screw-On Tri-Band Dipole (2 Supplied)

(U) The antennas are tri-band dipoles. Two SMA-style screw-on antennas come standard with the RM01 and provide omni-directional coverage in all modes of operation. These antennas are able to swivel and tilt to allow the relative position of the antennas to be changed, which can improve performance in some situations. The antennas should not be oriented such that they are touching each other.

2.2.2.3 (U) Antennas - External High-Gain (Optional)

(U) High-gain wall mount or mast-mount antennas are designed to be professionally installed and should abide by the FCC rules and regulations. Please install according to professional and proper installation requirements. The installers and end users should observe federal and local frequency authorizations and FCC part 15 for maximum Effective Isotropic Radiated Power (EIRP) and FCC limits (FCC 47 CFR part 1.1310) for Maximum Permissible Exposure.

2.3 (U) MODULE SETUP

(U//FOUO) The Cryptographic Module is designed to be combined with an external module to comprise one unit. Each module has controls and indicators to interface with the users and networks.

NOTE

(U) Refer to Section 2.2 for additional safety information regarding the setup and operation of the KIV-54 Cryptographic Module with an external module.

2.3.1 (U) KIV-54 Cryptographic Module Setup

(U//FOUO) The KIV-54 module requires no assembly. As part of the initial administrative setup, a Cryptographic Key or FIREFLY Vector (i.e., FIREFLY or Enhanced FIREFLY Vector) and P^3 dePAC Moduli must be installed in the KIV-54 prior to attaching an external module. The KIV-54 module is an unclassified Controlled Cryptographic Item (CCI) with a factory set security classification level of "Inhibit" until it is changed by the Administrator through the configuration Web pages. Only keys or vectors with the KIV-54's security classification level are accepted during the key installation process. The key is activated (as an administrative function) through the KIV-54 configuration Web pages.

2.3.1.1 (U) KIV-54 Cryptographic Module Status Indicators

(U//FOUO) KIV-54 status indicators are located on top of the module. When the power is applied to the KIV-54, all four status indicators (Light-emitting Diodes (LEDs)) are briefly illuminated to allow visual verification that the indicators are functional.

UNCLASSFIEID//FOUO

UNCLASSIFIED//FOUO

UNCLASSIFIED//FOUO

Status Indicator	State	Function
 PWR (green)	Not illuminated (Off)	Indicates power is Off.
	Blinking	Indicates power is applied and a boot-up is in progress.
	Steady (On)	Indicates power is applied and the boot-up process has completed.
 LINK (green)	Not illuminated (Off)	Indicates no Ethernet link is established.
	Blinking	Indicates Ethernet link activity.
	Steady (On)	Indicates Ethernet connectivity.
 FILL (yellow)	Not illuminated (Off)	Indicates a Key is loaded.
	Blinking	Indicates that no Key is loaded (i.e., needs Fill).
	Steady (On)	Indicates the Key Fill cable is attached.
 ALARM (red)	Not illuminated (Off)	Indicates that no fault has been detected.
	Blinking	Indicates the detection of a fault or after the panic zeroize buttons have been pressed while powered on.
	Steady (On)	When power is Off, indicates one or more of the following conditions: • A cover has been removed. • Panic Zeroize buttons are being pressed. When power is On, indicates that the cryptographic processor may have been tampered.

UNCLASSIFIED//FOUO

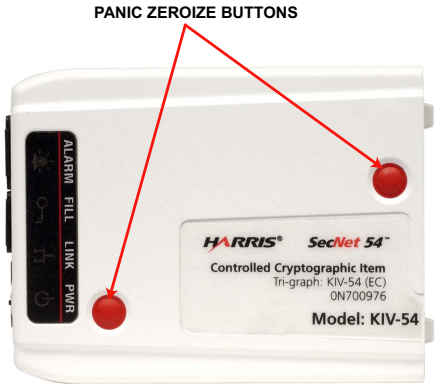
NOTE

(U//FOUO) When the ALARM LED is in the blinking state as a result of pressing the Panic Zeroize buttons with power On, the User must log off, power cycle the KIV-54RM01, and log back into the device to clear the fault.

2.3.1.2 (U) Panic Zeroize Buttons

(U//FOUO) The KIV-54 Panic Zeroize buttons are located on the top of the module.

UNCLASSIFIED//FOUO



UNCLASSIFIED//FOUO

UNCLASSIFED//FOUO

Control	Function
Panic Zeroize Buttons	Pressing the buttons simultaneously, while power is On or Off, causes the following conditions: • ALARM LED flashes if power is on. • ALARM LED is steady on if power is off. • Clears all stored cryptographic key data and associated PPK Chains and HAIPE® tunnel configurations. Note that Base and Alternate P³ dePAC Moduli are not deleted. • Clears all access control data. • Returns device security classification to Inhibit. • Returns the KIV-54 to its factory default state when power is cycled (i.e., turning the power Off and back On). • The ALARM LED flashes when the buttons are pressed.

UNCLASSIFED//FOUO

2-3.1.2.1 (U) Erase Cryptographic Keys (Zeroize)

(U//FOUO) Simultaneously, pressing the two red Panic Zeroize buttons on the KIV-54 while power is Off will erase all stored cryptographic key data (excluding dePAC Moduli) and reset the KIV-54 to the factory default configuration once it is power cycled. Refer to Section 2-3.1.2.2 for Factory Reset information.

- (U//FOUO) The red ALARM LED on the KIV-54 will illuminate steadily while the buttons are pressed.
- (U//FOUO) The ALARM LED will turn off when the buttons are released.

NOTE

(U//FOUO) Pressing the Panic Zeroize buttons, while power is “Off”, is an operation intended for use in a panic situation only. Since this process causes the ALARM LED to illuminate, it results in an additional drain on the internal backup battery, and if used repeatedly, will reduce the overall life of the battery.

NOTE

(U//FOUO) If KIV-54 power is on when the Panic Zeroize buttons are pressed, all stored configuration settings are erased in addition to the cryptographic key data and associated Key Chain (excluding dePAC Moduli) and HAIPE® tunnel configurations. Then, after power is cycled, the KIV-54 is reset to factory default configuration. Refer to Section 2-3.1.2.2 for Factory Reset information. (The ALARM LED will begin flashing when the buttons are pressed.)

(U//FOUO) Refer to Section 3.2.14 for information on Zeroizing the KIV-54 from the configuration Web pages.

2-3.1.2.2 (U) Factory Reset

(U//FOUO) The KIV-54 can be reset to the factory default configuration by pressing the two red Panic Zeroize buttons on the KIV-54 while the power is On or Off. The following factory default configuration is set when power is cycled:

- (U//FOUO) All cryptographic key data and associated PPK Chains (excluding dePAC Moduli) and tunnel configurations are erased.
- (U//FOUO) All stored configuration settings (including network configurations and external module configurations) are reset to the factory default values.
- (U//FOUO) All Administrator and User accounts are removed from login accounts, resetting to the factory default administrator account.
- (U//FOUO) Security classification level of the device is set to Inhibit.
- (U//FOUO) Active customer-developed Red SSL certificates (CA and Public/Private Key Pair) become inactive and Harris-developed SecNet 54® Red SSL certificates (CA and Public/Private Key Pair) become active.

(U//FOUO) Appendix F of this manual contains the KIV-54 factory default values. After factory reset, the power must be cycled on the KIV-54 (i.e., set the power switch to Off and then to On). After factory reset, the KIV-54 must be reconfigured by an Administrator before a User can use the device.

CAUTION

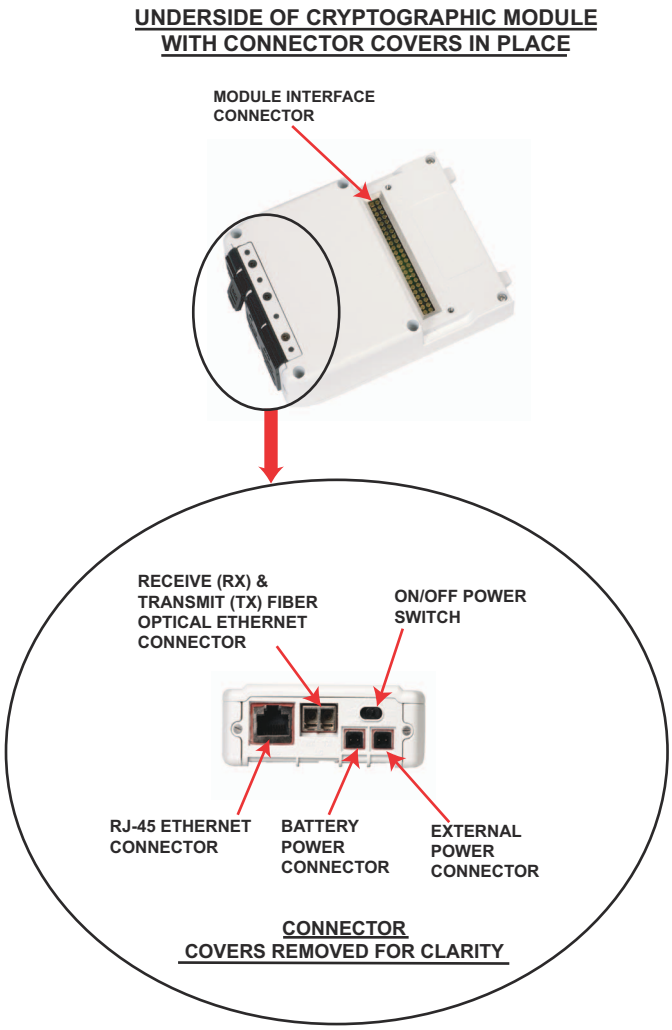
(U//FOUO) After factory reset, the KIV-54 may take several minutes to boot-up. Do not remove power from the KIV-54 while the boot-up is in progress.

(U//FOUO) A factory reset does not erase the audit log. All log entries remain until cleared by an Administrator.

2.3.1.3 (U) Power and Interface Connectors

(U//FOUO) Network and power connectors are located on the end of the KIV-54 module. Protective covers are used to seal out debris when network and power connectors are not in use. The module interface connector that connects to the external module is on the underside of the KIV-54 module.

UNCLASSIFIED//FOUO



UNCLASSIFIED//FOUO

UNCLASSIFIED//FOUO

Control or Connector	Function
On/Off POWER Switch	When the POWER switch is set to On, the KIV-54 goes into its power-on state. The power-on is approximately 1 minute. When the POWER switch is set to Off, the KIV-54 goes into its power-off state. Note that the power-off may take a few seconds to allow the audit log to complete.
Dual Power Connectors (Battery/ External (BATT/EXT))	This is the Direct Current (DC) power input that is supplied by an AC adapter (EXT) or an external battery (BATT). The EXT input has priority over the BATT input if both are attached. The input voltage range of the KIV-54 is 14-30 volts.
RJ-45 Ethernet Connector	This connector provides 802.3 wired Ethernet connection. The input is also able to provide power to the unit via 802.3af Power Over Ethernet (PoE) (red/classified/ plaintext side).
RX and TX Fiber Optical Ethernet Connector	This is an industry standard duplex multimode Lampert Connector (LC) receptacle that is compliant with IEEE 802.3u Fast Ethernet. This interface supports 100BASE-FX fiber networks.

UNCLASSIFIED//FOUO

NOTE

(U//FOUO) KIV-54 provides auto Medium Dependent Interface/Medium Dependent Interface Crossover (MDI/MDIX) capability and thus can operate from a standard or crossover Ethernet cable on its RJ-45 input connector.

CAUTION

(U//FOUO) Do not remove power from the KIV-54 by pulling out a power connector without first powering down the module using the power switch. Doing so could damage the KIV-54. When the KIV-54 is powering down, wait at least 10 seconds for LEDs to turn off.

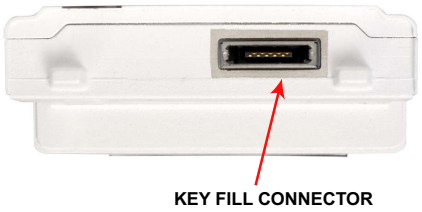
NOTE

(U//FOUO) If the ALARM LED blinks or illuminates steady before the PWR LED illuminates steady, the power cable must be disconnected to remove power from the KIV-54. The User must wait 30 seconds after the ALARM LED changes states (i.e., blinking or illuminating steady) before disconnecting the power cable.

2.3.1.4 (U) Key Fill Connector

(U//FOUO) The Key Fill connector is located on the end of the KIV-54 opposite the power connections. It is inaccessible when an external module is attached to the KIV-54. Key loading must be performed before connecting an external module. Key loading is preformed with Administrator login credentials.

UNCLASSIFIED//FOUO



UNCLASSIFIED//FOUO

UNCLASSIFIED//FOUO

Connector	Function
Key Fill Connector	Provides the connection for the DS 101 compatible Data Transfer Device (DTD). Provides the interface to load cryptographic key data.

UNCLASSIFIED//FOUO

2.3.2 (U) RM01 External Radio Module Setup

UNCLASSIFIED//FOUO

UNCLASSIFIED//FOUO

2.3.2.1 (U) Attaching the Antennas to RM01

(U) Perform the following procedure to attach the antennas to the RM01 module.

1. (U) Insert the hinged tri-band antenna into the RM01 SMA connector (refer to Section 2.3.2.3); position antenna in an upright position; and while holding the body of the antenna, turn the threaded portion until tight.

CAUTION

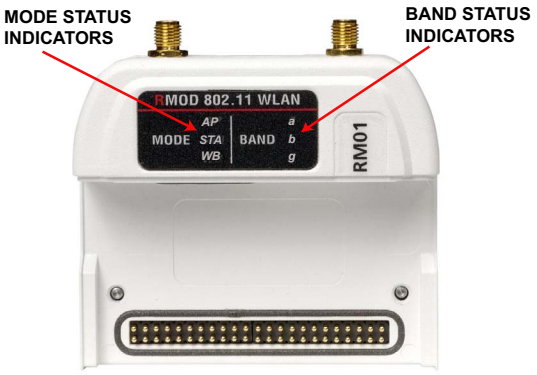
(U//FOUO) Do not over-torque the SMA antenna when attaching to RM01 radio module. Do not spin the body of the antenna around while tightening.

2. (U) Repeat Step 1 for second antenna.

2.3.2.2 (U) RM01 Status Indicators

(U//FOUO) During operations, the MODE status LEDs indicate the operational mode of the radio, and the BAND status LEDs indicate the frequency band. When all status LEDs are off (not illuminated), the radio is disabled and cannot transmit or receive. The following figure illustrates and Sections 2-3.2.2.1 and 2-3.2.2.2 describe each of the MODE and BAND status LEDs.

UNCLASSIFIED//FOUO



UNCLASSIFIED//FOUO

2-3.2.2.1 (U) 802.11 WLAN MODE LEDs

UNCLASSIFIED//FOUO

Indicator	State	Function
AP LED (green) STA LED (yellow) WB LED (green)	None illuminated (Off)	Indicates power is Off or the RM01 is in the disabled state.
	All three simulta-neously illumi-nated and blinking	Indicates RM01 is booting up after being enabled.
	One blinking	Indicates RM01 is booting up after a con-figuration change. (Radio boot up can take up to 30 seconds.)
	One illuminated	Indicates boot process is complete and the RM01 is operating in the indicated mode.

UNCLASSIFIED//FOUO

2-3.2.2.2 (U) 802.11 WLAN BAND LEDs

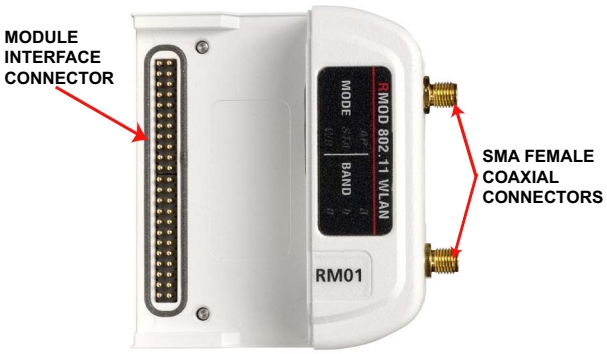
UNCLASSIFIED//FOUO

Indicator	State	Function
a LED (green) b LED (yellow) g LED (green)	None illuminated (Off)	Indicates one of the following conditions: • The power is Off. • The RM01 radio is in the disabled state. • The RM01 radio is configured as an infrastructure station and is not associated with an Access Point (AP).
	All 3 blinking	Indicates the RM01 radio boot up is in process after the radio has been enabled. (Radio boot up process can take up 30 seconds.)
	One blinking	Indicates operating band. Note the following: • During link activity, the blink rate is proportional to activity. • For an infrastructure station, the band LED blinks only after associating with an AP. • g LED indicates b/g operating band.

UNCLASSIFIED//FOUO

2.3.2.3 (U) RM01 Interface Connectors

UNCLASSIFIED//FOUO



UNCLASSIFIED//FOUO

UNCLASSIFIED//FOUO

Connector	Function
Module Interface Connector	This connector provides the power and data interface to the RM01 via the KIV-54.
SMA Female Coaxial Connectors	The antenna connections.

UNCLASSIFIED//FOUO

2.4 (U) RM01 OPERATIONAL CONFIGURATION

(U//FOUO) The RM01 can be configured for use as an IEEE 802.11a, 802.11b, or 802.11g wireless network. The 802.11b mode uses Direct Sequence Spread Spectrum (DSSS) transmission, the 802.11a mode uses Orthogonal Frequency Division Multiplexing (OFDM) transmission, and the 802.11g mode uses both the DSSS and OFDM transmissions. In addition, the RM01 uses highly integrated mixed-signal Complementary Metal-oxide-semiconductor (CMOS) technology exclusively for the wireless chipset, minimizing power consumption while maximizing reliability.

(U//FOUO) To maximize operating distance and to minimize having different antennas for each frequency band, the RM01 uses a tri-band omni antenna with 0 dBi gain.

(U//FOUO) The significant features of the RM01 radio are as follows:

- (U//FOUO) Dual-Band, Multimode WLAN Radio
  - 802.11b, DSSS, 2.4 GHz ISM Band, 1 to 11 Mbps data rates
  - 802.11g, DSSS/OFDM, 2.4 GHz ISM Band, 1 to 54 Mbps data rates
  - 802.11a, OFDM, 5 GHz Lower and Upper UNII Band, 6 to 54 Mbps data rates

- (U//FOUO) Selectable transmit power settings
- (U//FOUO) Antenna Ports with SMA female connectors
- (U//FOUO) Receive Antenna Diversity

2.5 (U) RM01 ENVIRONMENTAL CHARACTERISTICS

(U) This section provides general guidelines on factors that influence RF network performance.

2.5.1 (U) Site Survey

(U) Because of differences in component configuration, placement and physical environment, every network application is a unique installation. Before installing the system, a survey of the site should be performed to determine the optimum utilization of networking components and to maximize range, coverage, and network performance.

(U) Several environmental situations and operating conditions should be considered when setting up a network. These situations and conditions are included in the following sections.

2.5.2 (U) Antenna Placement

(U) To maximize the RM01 range, it is very important to set up the proper antenna configuration. Range usually increases in proportion to antenna height and orientation. Experimentation may be necessary to determine the optimum antenna height and orientation. Start by placing the antennas in a 45 degree “rabbit ear” orientation. The antennas should not be pointed toward each other or touch each other.

2.5.3 (U) Data Transmission Rates

(U//FOUO) Since data bit rates are inversely proportional to sensitivity and range, maximum radio range is achieved at the lowest workable data rate (e.g., 1 or 2 Mbps). As the radio data rate increases, the receiver threshold sensitivity decreases, thereby decreasing range. The RM01 provides a bit rate setting of “BEST”, which will automatically adjust the bit rate to match the existing conditions.

2.5.4 (U) Obstructions, Building Materials

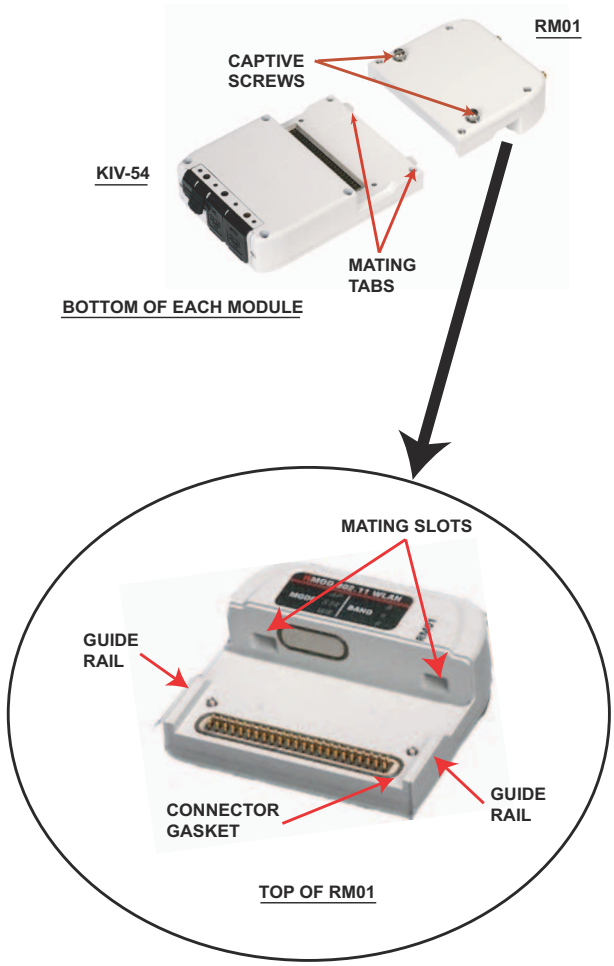
(U) Obstructions like steel pillars, thick concrete walls and metal cabinets and shelving can hinder the performance of the RM01. Avoid locating the device and antennas in a location where there are barriers like these between the sending and receiving antennas. Since the penetration of radio signals is greatly influenced by the types of building materials used in construction, it is important to know what the structures are made of that surround or border the transmitting and receiving equipment. Drywall and plywood construction, for example, allows greater range than does metallic walls or concrete blocks. Metal and steel construction usually impedes radio signals. In some cases, windows can improve coverage to other floors with windows.

2.6 (U) ATTACHING AN EXTERNAL MODULE TO THE CRYPTOGRAPHIC MODULE

2.6.1 (U) General Information

(U//FOUO) The following procedure describes how an external module is attached to the KIV-54. The following figure indicates connection points on each unit.

UNCLASSIFIED//FOUO



UNCLASSIFIED//FOUO

CAUTION

(U//FOUO) There are no operator serviceable components within the KIV-54. Do not attempt to remove the KIV-54 covers.

CAUTION

(U//FOUO) Ensure that the Cryptographic Module power is Off when attaching an external module.

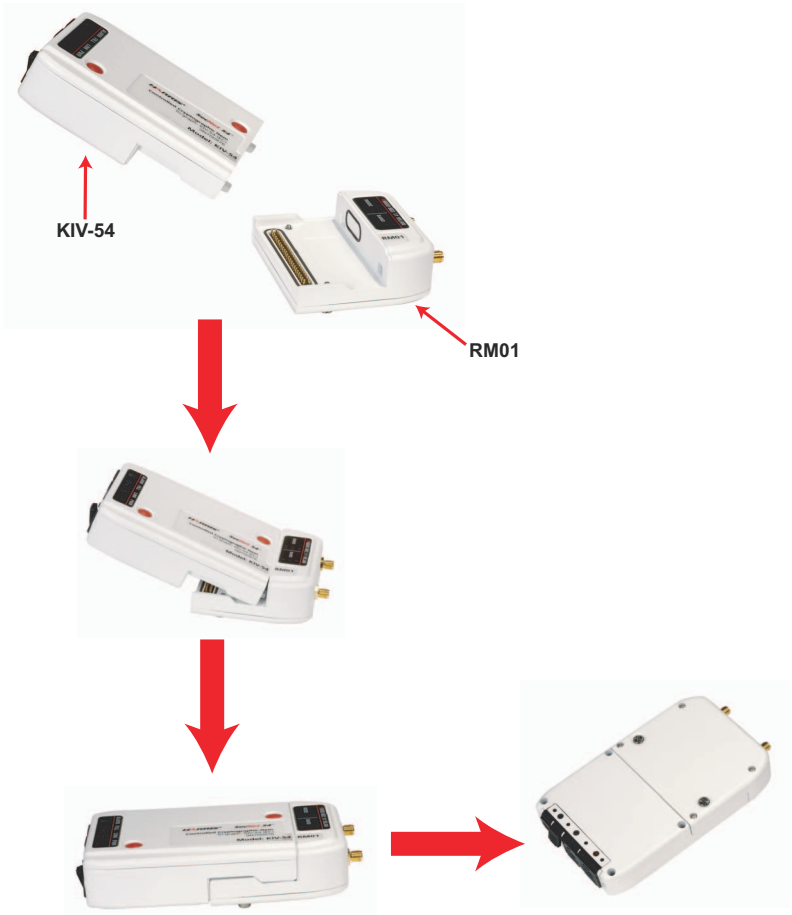
NOTE

(U//FOUO) Loading the Cryptographic Key or FIREFLY Vector and dePAC Moduli are required prior to connecting the units. Key loading is performed with Administrator login credentials.

(U//FOUO) To attach the RM01 Radio Module to the KIV-54 Crytographic Module, refer to the following illustration and perform the following procedure.

1. (U//FOUO) With both units facing upward, position the KIV-54 on top of the XMOD, then tilt and insert mating tabs on KIV-54 into mating slots in XMOD.

UNCLASSIFIED//FOUO



UNCLASSIFIED//FOUO

2. (U//FOUO) While firmly holding the modules together, turn the modules over to access the captive screws in the XMOD.

3. (U//FOUO) Hold both modules securely while tightening the two screws (screws are spring-loaded).

2.7 (U) CONNECTING POWER TO THE KIV-54 CRYPTOGRAPHIC MODULE

NOTE

(U//FOUO) Power should not be attached to the KIV-54 module while the power switch is in the On position.

2.7.1 (U) DC Power

(U//FOUO) When power is applied to the KIV-54, the KIV-54 supplies power to the external module (such as a RM01 radio module). The KIV-54 has two DC input connectors marked EXT and BATT (refer to the figure in Section 2.3.1.3). The EXT connector is intended to be used with the supplied external power supply, while the BATT input is intended to be used with an external battery (not supplied).

(U//FOUO) The operating voltage range of the DC input is 14V - 30V. The KIV-54 prioritizes the two DC input connectors with the one labeled EXT being of higher priority. This prevents battery drain when the KIV-54 is connected to the AC power supply. A battery can be connected to the BATT connector for use as an Uninteruptable Power Source (UPS) in the event of a temporary power outage.

2.7.2 (U) Power over Ethernet (PoE)

(U//FOUO) The KIV-54 is capable of operation from a PoE Ethernet connection on the RJ-45 input and is compatible with the IEEE 802.3 af PoE specification. Thus, with a PoE enabled Ethernet connection, no connection is necessary to the two DC input connectors, although an external battery connection could be used to provide an UPS function as described in the section above.

NOTE

(U//FOUO) In the presence of PoE, the following priorities are in effect:

1. (U//FOUO) When both PoE and a connection to the EXT connector exist, the KIV-54 and connected XMOD will operate from the EXT connection.

2. (U//FOUO) When both PoE and a connection to the BATT connector exist, the KIV-54 will operate from PoE.

CAUTION

(U//FOUO) Do not unplug power from the EXT connector while PoE is available on the wired Ethernet connection without first turning the power switch to the Off position. Otherwise, the device may not transition smoothly to PoE and may power down momentarily.

NOTE

(U//FOUO) When a battery is used as the only power source, the battery can be changed by plugging a fresh battery into the unused (EXT or BATT) connector before removing the depleted battery. Following this procedure will not disrupt communications. This procedure does not work if PoE is provided by the wired Ethernet connection.

2.8 (U) ATTACHING THE KIV-54 TO THE NETWORK

(U//FOUO) The KIV-54 has both wired (RJ-45) and optical Ethernet connectors. The two connection types are provided for flexibility. The KIV-54 does not support simultaneous connection to two networks.

2.8.1 (U) Wired Ethernet Connection

1. (U) Refer to the illustration in Section 2.3.1.3 for KIV-54 interface connector locations.

2. (U//FOUO) Connect the Ethernet Red cable from the network to the RJ-45 connector on the KIV-54.

NOTE

(U//FOUO) KIV-54 provides auto MDI/MDIX capability and thus can operate from a standard or crossover Ethernet cable on its RJ-45 input connector.

2.8.2 (U) Optical Ethernet Connection

1. (U) Refer to the illustration in Section 2.3.1.3 for KIV-54 interface connector locations.

2. (U//FOUO) Connect a Fiber cable (not supplied) from the network to the LC RX and TX Fiber connector on the KIV-54. The KIV-54 transmits on the side marked TX and receives on the side marked RX.

2.8.3 (U) Ethernet Connection Considerations

(U//FOUO) At power-on the KIV-54 continuously scans back and forth between the wired and optical Ethernet interfaces until it finds the one with a link. Once a link is discovered, it becomes active and data on the other interface is ignored. Once the active link is severed, the device scans both interfaces looking for a link again.

(U//FOUO) If both the wired and optical Ethernet interfaces have a link at power-on, the optical interface will be used for data (active link).

NOTE

(U//FOUO) If a wired Ethernet cable with PoE is plugged in while the optical Ethernet interface data link is in use, PoE can supply power, but data on the wired Ethernet interface is ignored. Refer to Section 2.7.2 for information on PoE constraints.

NOTE

(U//FOUO) Disconnecting the Ethernet cable from the KIV-54 will log a user out of the configuration Web pages for that device and place the RM01 in the adjusted state. When the Ethernet cable is plugged back into the device and the link is established, the User can refresh the Web page and continue device configuration.

2.9 (U) USING THE KIV-54RM01 OUTDOORS

(U) When using the KIV-54RM01 outdoors, the device should be oriented in the vertical position with the antennas at the top and the connectors and cables at the bottom. This should prevent water from penetrating the device in case of rain. If Users plan to operate the device in extreme environmental conditions, a suitable environmental enclosure should be used to encase the device.

Chapter 3

(U) DEVICE CONFIGURATION AND MONITORING

3.1 (U) CHAPTER CONTENTS

(U//FOUO) This chapter contains information about and configuration Web pages embedded within the SecNet 54 device (i.e., KIV-54RM01). A standard Web browser is used to access configuration Web pages. The privileges associated with the login credentials control the items that can be configured.

(U//FOUO) Although both the Administrator and User have privileges to access the configuration Web pages, this User manual illustrates and describes configuration Web pages and their associated functionality that are applicable to the login credentials of a User.

(U) The chapter details include the following:

- (U) Selecting and viewing the SecNet 54® Secure Socket Layer (SSL) Server and SSL Client Certificates
- (U) Logging into the Configuration Web pages
- (U) Viewing the current cryptographic status of the SecNet 54® device and status of the attached XMOD
- (U) Viewing status of the SecNet 54® High Assurance Internet Protocol Encryptor (HAIPE) Red and Black networks
- (U) Configuring the RM01 External Radio Module (RMOD)
- (U) Viewing the Security Classification Level and Traffic Flow Security (TFS) parameters
- (U) Loading and viewing the customer-developed Red SSL Security Certificates (Certification Authority (CA) and Public/Private Key Pair) and Black Security Certificates (Wi-Fi Protected Access 2 (WPA2) CA, WPA2 Private/Public Key Pair, and Virtual Private Network (VPN))
- (U) Viewing the cryptographic Pre-Placed Keys (PPKs), PPK Chains, FIREFLY Vectors, and P^3 dePAC Moduli
- (U) Viewing HAIPE® tunnels and Dynamic Discovery Communities of Interest (COI)
- (U) View Routing Information Protocol version 2 (RIPv2) configuration for Red-side Routing and view Red Routing Table
- (U) Changing the User Passwords
- (U) Viewing and exporting audit log events
- (U) Logging out of the Configuration Web pages
- (U) Rebooting the device
- (U) Zeroizing the device

3.2 (U) CONFIGURATION WEB PAGES

(U//FOUO) The KIV-54 contains an embedded Web server and Web pages that are used to configure SecNet 54® device settings. The embedded configuration Web pages within the KIV-54 are accessed directly from a Web browser running on a Red network computer.

NOTE

(U//FOUO) For SecNet 54® device configuration, the computer's Web browser must meet the following minimum requirements:

- (U) CSS 2.1 and HTML 4.01 must be supported
- (U) JavaScript must be enabled
- (U) Cookies must be enabled
- (U) Support SSL/Transport Layer Security (TLS)

3.2.1 (U) SSL Certificates

(U//FOUO) The KIV-54 uses SSL certificates to ensure a secure Web browser connection during the configuration session. The SSL certificates ensure two-way authentication with both a server side certificate (i.e., SecNet 54® SSL CA) and client side certificate (i.e., SecNet 54® SSL Client). The SSL Certificates are signed by the SecNet 54® CA. The SecNet 54® CA is added to the Trusted Certification Authorities in each Web browser that needs to connect to the SecNet 54® devices. Adding the SecNet 54® CA allows the Web browser to trust the SecNet 54® devices. The SSL Client Certificate must match the Server Certificate for the HTTPS server to allow the browser to proceed. If it does not match, the server terminates the SSL connection and the browser will not open.

NOTE

(U//FOUO) Prior to accessing the KIV-54 configuration Web pages, the SecNet 54® SSL Server and Client Certificates must be loaded into the local computer using a Web browser. The Harris-developed SecNet 54® SSL Certificates are located on the SecNet 54® Applications CD (refer to Section 1.3.1). If using more than one Web browser, the SSL Certificates must be installed for each browser.

(U//FOUO) Once the certificates have been loaded into the local computer for a specific Web browser, reinstallation of the certificates is not necessary during the login process. The KIV-54 will negotiate up to AES 256-bit encryption and will also work with browsers that use lower level encryption. Appendix G describes importing the SecNet 54® SSL Certificates into three common Web browsers, IE, Mozilla Firefox, and Netscape.

3.2.2 (U) Initiating the Login Process

(U//FOUO) Logging into the SecNet 54® configuration Web pages is accomplished through the computer's Web browser. The User enters the device's IP address as the Uniform Resource Locator (URL) into the Web browser Address bar (or Location bar) to display the **DEVICE LOGIN** window. The URL that is entered must be a Hypertext Transfer Protocol Secure (HTTPS) address (i.e., https://192.xxx.x.xx) instead of a plain HTTP. Failure to include a secure HTTPS entry will result in an error message that is applicable

to the Web browser being used. The IP address (i.e., the URL) for the User's SecNet 54® device is obtained from the Administrator.

Entering the appropriate IP address initiates the login process, and the window displayed is browser dependent. To ensure the Web pages are displayed in a specific Web browser, the browser must be set as the operating system's default browser for that computer.

Sections 3.2.2.1 and 3.2.2.2 describe selecting the appropriate SecNet 54® SSL Certificate to access the SecNet 54® configuration Web pages using IE and Mozilla Firefox Web browsers when they are set as the default Web browsers. Refer to Section 3.2.1 for information about the SecNet 54® SSL Certificates and Appendix G for Web browser certificate installation instructions.

NOTE

(U//FOUO) If the Red SSL Server or Client certificate is expired, an error will display in the Web browser window and disallow login into the configuration Web pages. Refer to Section TBD for browser specific steps that allow the use of an expired trusted certificate.

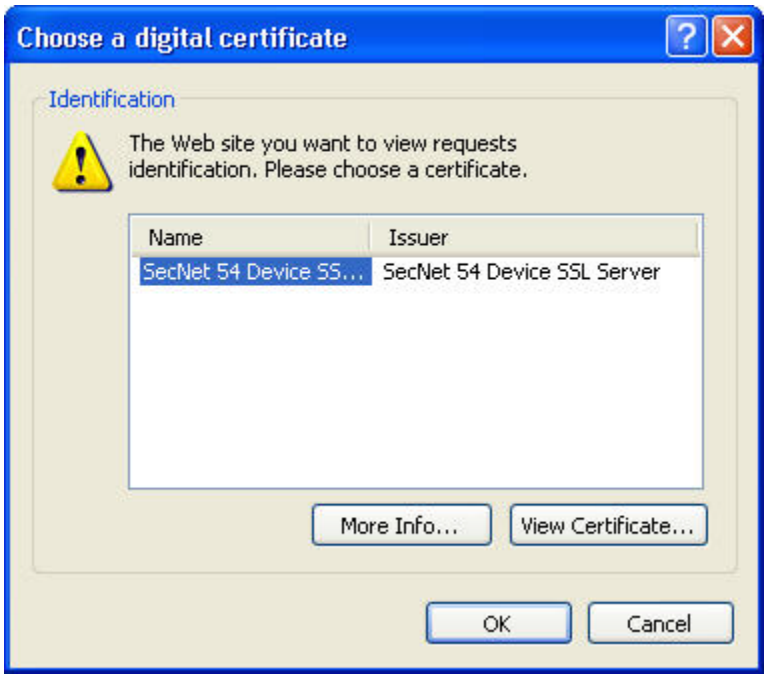
3.2.2.1 (U) Using the IE Web Browser to Access Device Configuration Settings

(U//FOUO) When the device's IP address is recognized, the **Choose a digital certificate** window displays.

NOTE

(U) The following certificates and associated data are examples. The actual certificate dates and associated data may differ when certificates are revised.

UNCLASSIFIED//FOUO



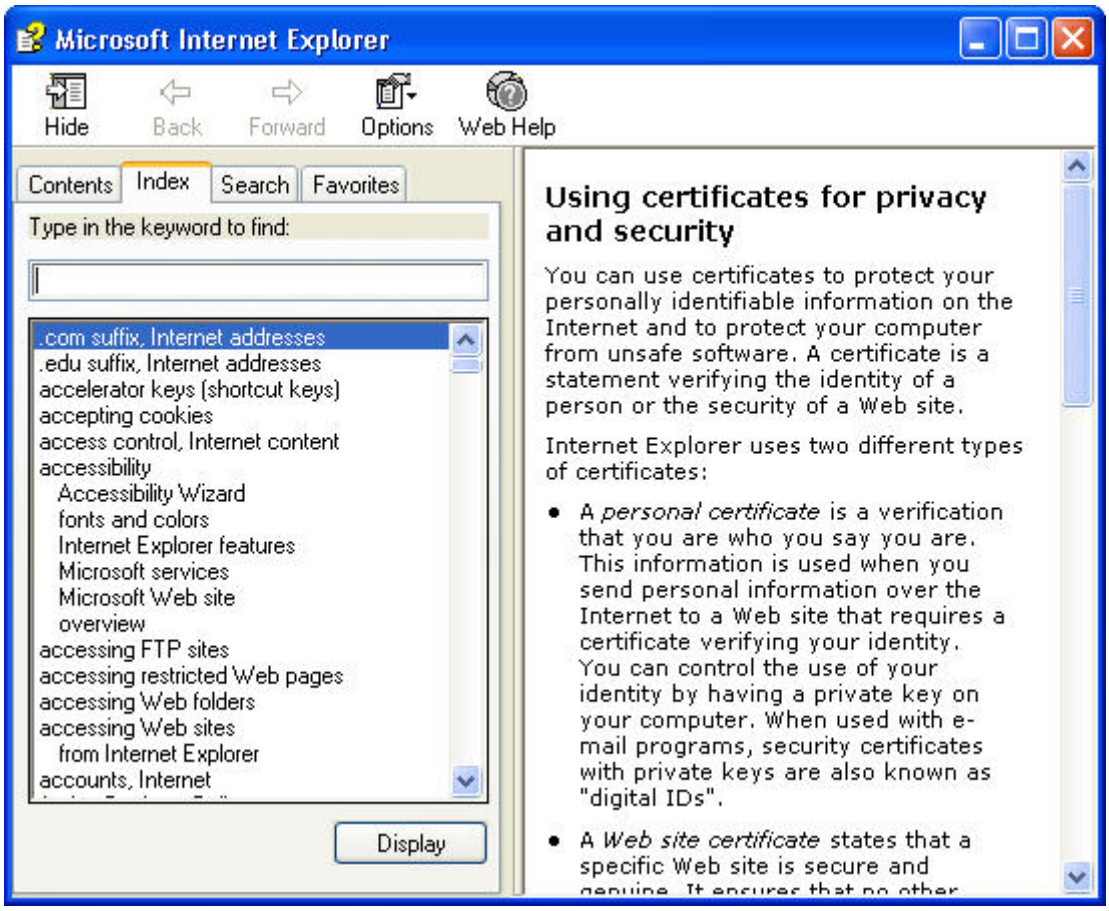
UNCLASSIFIED//FOUO

(U//FOUO) From this window, the User accesses information about digital certificates and views specific information about the selected SecNet 54® SSL Certificate.

(U//FOUO) Selecting the **More Info...** button displays the computer's default Web browser's "Help" information about certificates. The **View Certificate...** button selection displays the selected digital SecNet 54® SSL Certificates. The SecNet 54® SSL Server and Client Certificates must be installed to connect to a secure Web browser. Refer to Section 3.2.1 for information about the certificates and Appendix G for Web browser certificate installation instructions. The browser Help window and the **Certificate** window are illustrated below.

(U//FOUO) The **Cancel** button selection removes the **Choose a digital certificate** window and the Web pages are not displayed, indicating that a connection cannot be made. Selecting the **OK** button displays a **Security Alert** window (i.e., if the default Web browser is IE), which once acknowledged (i.e., the **Yes** button selection), launches the host computer's default Web browser to access device configuration settings. This security window is illustrated before the Certificate window.

UNCLASSIFIED



UNCLASSIFIED


Certificate
General
Details
Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
•All application policies
Issued to: SecNet 54 Device SSL Client Certificate
Issued by: SecNet 54 Device SSL Server
Valid from 12/31/1999 to 12/31/2037
You have a private key that corresponds to this certificate.
Issuer Statement
OK

UNCLASSIFIED

The **DEVICE LOGIN** window is displayed after **Yes** is selected from the **Security Alert** window. Refer to Section G.5.1for additional information about the **Security Alert** window and acknowledging additional browser security warnings and alerts and Section 3.2.2.3 for a description of the **DEVICE LOGIN** window.

3.2.2.2 (U) Using the Mozilla Firefox Web Browser to Access Device Configuration Settings

NOTE

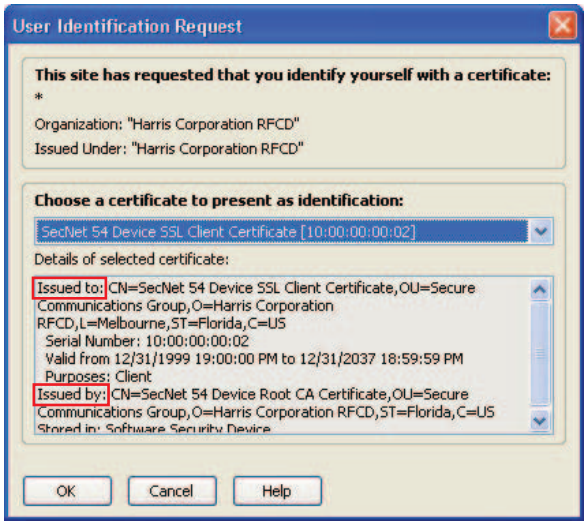
(U) The following certificates and data are examples. The actual certificate dates and associated data may differ when certificates are revised.

(U//FOUO) When the device's IP address is recognized, the **User Identification Request** window is displayed. From this window the User accesses information about digital certificates and provides identification by selecting a certificate.

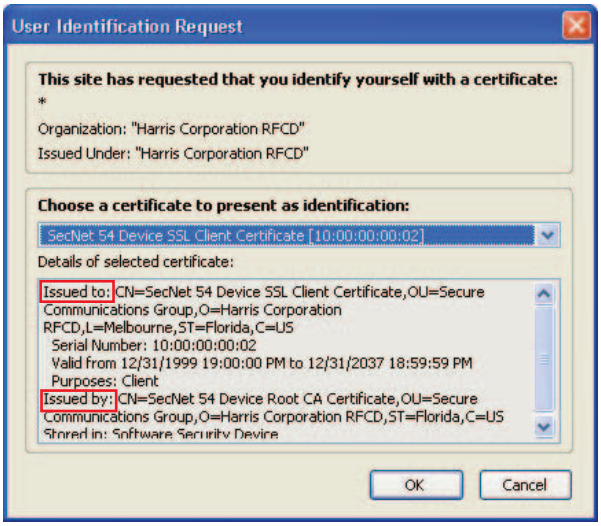
NOTE

(U//FOUO) To ensure that the **User Identification Request** window displays, select the "Ask Every Time" or "Ask me every time" radio button from the **Options** window as described in Section G.3.1 or G.3.3 when loading certificates into the Mozilla Firefox Web browser. Failure to select this option may display an error message and prevent login to the SecNet 54® configuration Web pages.

(U) The following figure illustrates the **User Identification Request** windows for Mozilla Firefox Web browsers versions 1.0.x and 1.5.x.



Web Browser Mozilla Firefox 1.0.X



Web Browser Mozilla Firefox 1.5.X - 3.0.X

(U//FOUO) The down arrow selection in the **Choose a certificate to present as identification** area displays each certificate with associated details below the selection. Viewing the “Issued to” and “Issued by” information in the bottom area indicates if the certificate selected is for the “SecNet 54® Device”. The SecNet 54® SSL Certificate must be selected from this window for each login to the SecNet 54® configuration Web pages.

(U) When the **User Identification Request** window is displayed from the Mozilla Firefox Web browser, version 1.0.x, three buttons are displayed on the window, **OK, Cancel**, and **Help**. Refer to the previous

figure. When accessing the **User Identification Request** window from the Mozilla Firefox Web browser, version 1.5.x, two buttons are displayed on the window, **OK** and **Cancel**. Selecting the **Help** button (version 1.0.x) displays help for Mozilla Firefox, and selecting the **Cancel** button (versions 1.0.x and 1.5.x) removes the **User Identification Request** window and redisplays it. Reselecting the **Cancel** button removes the window and displays an error message.

(U) Selecting the **OK** button from the **User Identification Request** window (versions 1.0.x and 1.5.x) displays a **Prompt** to enter a master password for the security device, as illustrated in the following figure. However, if a master password has not been defined (as described in Section G.3.2) when installing the SSL Client Certificate, this prompt will not appear.

UNCLASSIFIED

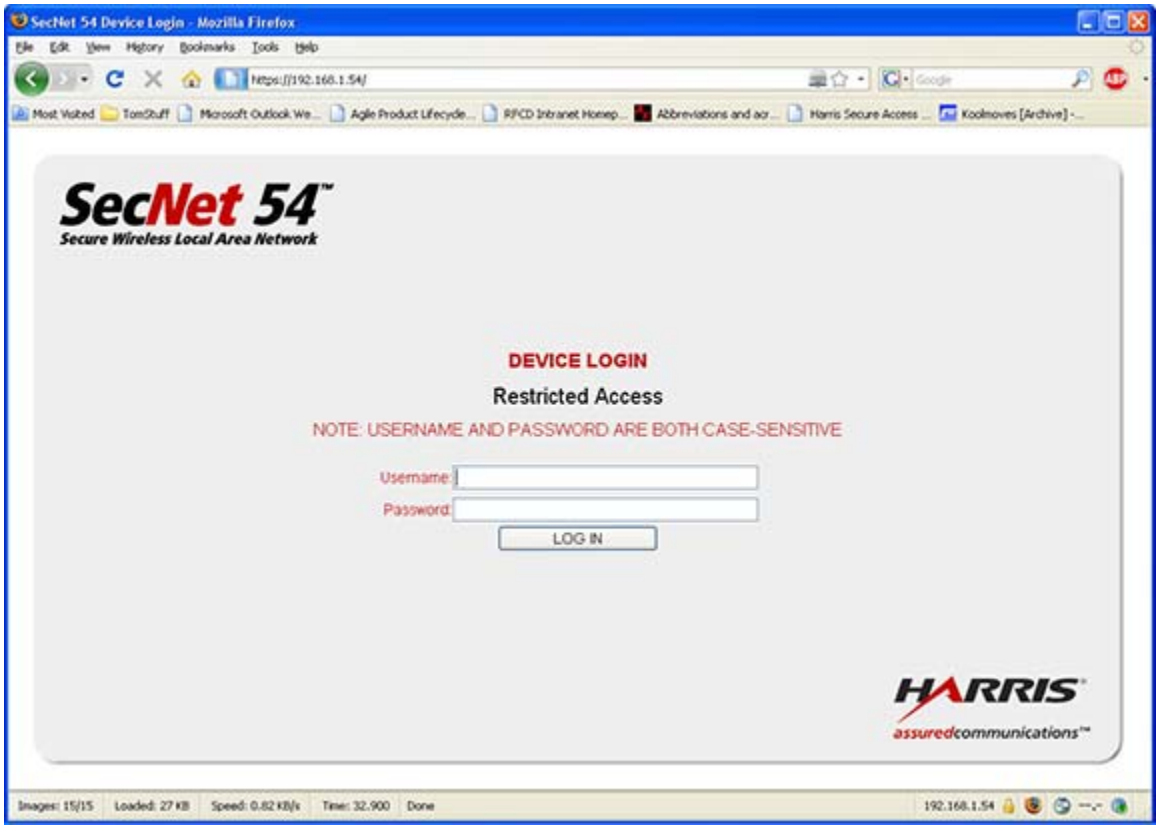
UNCLASSIFIED

(U//FOUO) In this example the password for the SecNet 54® device is **secnet54** in all lowercase letters. The **OK** button selection confirms the password and displays the SecNet 54® **DEVICE LOGIN** window (refer to Section 3.2.2.3). The **Cancel** button selection removes the window and displays an error message.

3.2.2.3 (U) Logging into the Configuration Web Pages

(U//FOUO) The **DEVICE LOGIN** window is displayed after acknowledging Web browser security alert messages (Section G.5) when accessing SecNet 54® Web pages directly from the secure browser (3.2.2).

UNCLASSIFIED//FOUO



UNCLASSIFIED//FOUO

(U//FOUO) Access to the SecNet 54® Configuration Web pages is restricted to Administrators and Users with valid login credentials for the device. The privilege level associated with the supplied credentials (Administrator or User) controls the configuration settings which can be accessed.

(U//FOUO) Each KIV-54 contains its own embedded Access Control List (ACL) which holds the Administrator and User login credentials for the device. The login credentials consist of a Username and Password. Access to the ACL is provided with an Administrator login.

(U//FOUO) The KIV-54 is shipped from the factory with only default Administrator login credentials. This section describes the login process used for subsequent logins to the same device.

NOTE

(U//FOUO) After 10 minutes of inactivity, the Web server automatically logs a User out of the configuration Web pages and displays the following **Session Timeout** page. Selecting the page's hyperlink allows the User to re-enter their credentials via the **DEVICE LOGIN** page.

UNCLASSIFIED//FOUO

UNCLASSIFIED//FOUO

NOTE

(U//FOUO) If the SecNet 54® ALARM LED is illuminated while attempting to login and the login fails, the device should be rebooted and the login repeated. However, if the alarm condition continues and the login continues to fail, the device must be sent back to the manufacturer for repair.

NOTE

(U//FOUO) Web browsers can be configured to cache (auto-complete function) the values in specific fields, including the login credentials. Check the configuration of the installed Web browser. To protect the login credentials, ensure that the auto-complete function (cache) is turned off. An enabled auto-complete function may seriously compromise the security of the login credentials. This is a Web browser feature that Harris cannot control.

(U//FOUO) **Username** and **Password** are entered in the fields provided on the **DEVICE LOGIN** Web page. Selecting the **LOG IN** button submits the credentials to the device for validation. Only username and password combinations previously entered into the device's ACL are valid. After validation of the entered username and password, the main Configuration Web page is displayed.

(U//FOUO) A User account is allowed two (2) failed login attempts. The third (3rd) failed login attempt results in the User being locked out of the device. The User's credentials are no longer valid on that device. An Administrator can reset the User's credentials, allowing the User to regain access to the device.

To provide new credentials the Administrator deletes the current User account and creates a new account for the User.

(U//FOUO) To ensure confidentiality, new Users (as defined by the Administrator) must change their passwords upon initially logging into the SecNet 54® Configuration Web pages. Refer to Section 3.2.11.2 for information on changing the User password.

3.2.2.4 (U) Simultaneously Logging into a SecNet 54® Device

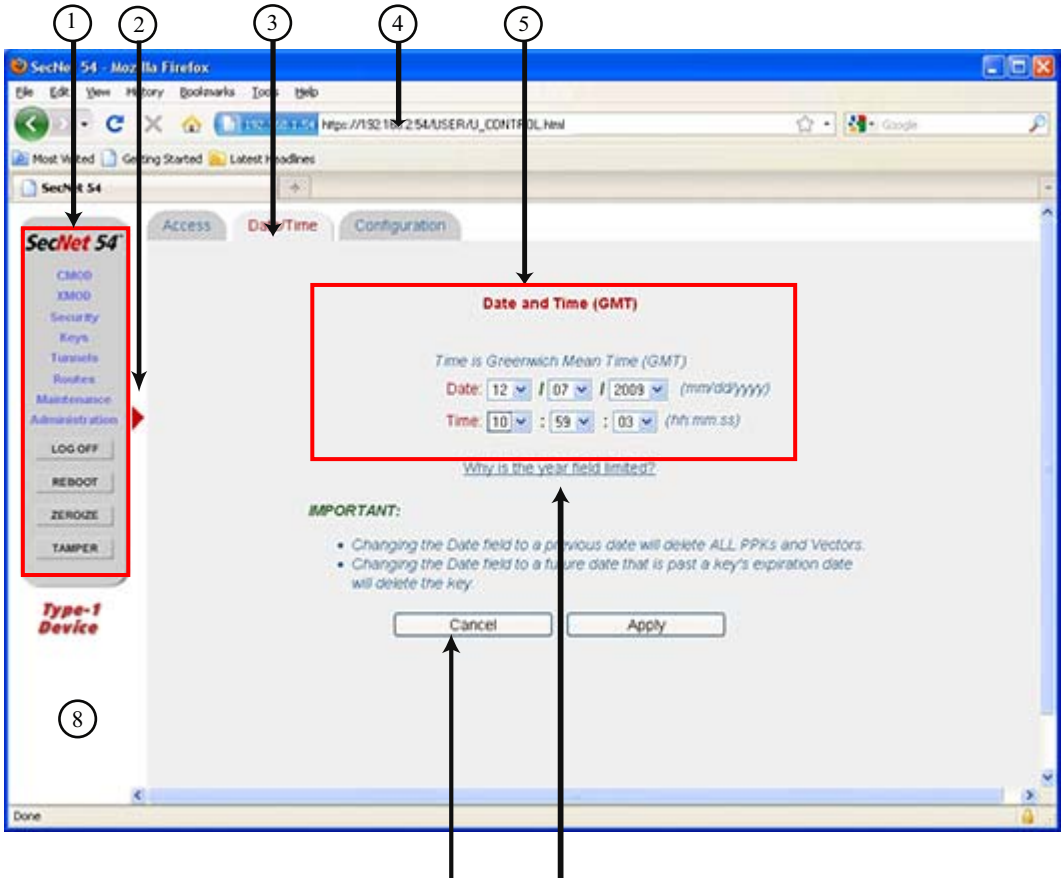
(U//FOUO) Only one User or Administrator can log into a device at a time. When two or more Users (or Administrators) attempt to simultaneously log into the same device, only one User or Administrator is allowed to log in and the others will receive an error message indicating that the device has reached its maximum user limit.

3.2.3 (U) Configuration Web Page Components

(U//FOUO) Once the Login has completed successfully, the configuration Web page is displayed with a menu bar down the left side and tabbed pages on the right. The **CMOD** menu bar option, displaying the **Current Status** page, is the selected default. The following figure is an example of a Web page status window with the components of the Web page described in the table following the figure.

(U//FOUO) An Alarm Status Area, located below the menu bar and device type, displays device errors and alerts. When no device errors or alerts have occurred, the Alarm Status area is blank, as illustrated in the figure below.

UNCLASSIFIED//FOUO



UNCLASSIFIED//FOUO

UNCLASSIFIED//FOUO

Call out	Component	Description
1	Menu Bar	The menu bar contains menu options that provide access to sets of configuration Web pages. It also contains four option buttons for performing operations on the device. Refer to Section 3.2.4 for a description of functions associated with menu bar options and option buttons.
2	Menu Bar Pointer	The Pointer moves up and down to indicate the selected menu bar option, which provides access to the set of associated configuration pages.

Call out	Component	Description
3	Page Tab	Selecting the page tab displays the page associated with the active menu option. Note that the tab's title text is the active link for selecting a page.
4	Address Bar or Location Bar	The Address bar or Location bar displays the URL of the device to be configured in the Web browser. The URL entered must be a secure HTTPS address.
5	Status and Data Entry Area	Current status values and configurable input fields are displayed in this area.
6	Hyperlink Text	The selection of this text displays the linked SecNet 54® configuration Web page.
7	Option Button	The selection of a Web page option button initiates an operation.
8	Alarm Status Area	The Alarm Status Area displays information about device alerts and errors. This area also indicates that the device is Type-1 (cryptographic).

UNCLASSIFIED//FOUO

NOTE

(U//FOUO) The SecNet 54® menu bar, on the left side of the screen, and the page tabs allow the User to navigate through the SecNet 54® configuration Web pages. However, the Web browser navigation tools at the top of the browser window are not associated with SecNet 54® functionality and are not used for managing the device.

NOTE

(U//FOUO) After 10 minutes of inactivity, the Web server automatically logs a User out of the configuration Web pages and displays a **Session Timeout** page (refer to figure in Section 3.2.2.3). Selecting the page's hyperlink allows the User to re-enter credentials on the **DEVICE LOGIN** page.

3.2.4 (U) Selecting Configuration Menu Bar Options

(U//FOUO) The SecNet 54® menu bar is a vertical bar on the left side of the configuration Web page. The menu options all have a corresponding set of selectable tabs that provide access to the associated configuration Web pages. The **LOG OFF**, **REBOOT**, and **ZEROIZE** option buttons are selected to perform operations on the actual device. The following tables list and describe menu bar options, their associated tabs, and menu bar option buttons.

UNCLASSIFIED//FOUO

Menu Bar Option	Selectable Tab and Function
CMOD	CURRENT STATUS • Display device status • Clear device alerts HAIPE® NETWORK • Display Red and Black Network Status
XMOD	RM01 • Display Wireless Settings Status • Configure Settings • Enable/Disable Communications • Reset to Default Settings WIRELESS SECURITY SETTINGS • Configure Wireless Security Settings VPN SECURITY • Display General RMOD Virtual Private Network (VPN) Status • Connect/Disconnect VPN Tunnel • Display RMOD VPN Authentication Method • Display RMOD Phase 1 Status • Display RMOD Phase 2 Status • Configure Settings • Renew DHCP lease • Reset Default Settings SEND PING • Ping another device on the black network • Display ping results

Menu Bar Option	Selectable Tab and Function
Security	CLASSIFICATION LEVEL • Display status TRAFFIC FLOW SECURITY • Display status CERTIFICATES • Install Red SSL Certificates (for Web access) • Install Black Certificates (WPA2 CA, WPA2 Public and Private Key Pair, and VPN) • View installed Red Certificates • View installed Black Certificates
Keys	PRE-PLACED KEYS • Display PPKs PPK CHAINS - SUMMARY • Display PPK Chain name and associated chain information FIREFLY VECTOR • Display FIREFLY Vectors and associated information P^3 DEPAC MODULI • Display Base and Alternate P^3 dePAC Moduli
Tunnels	TUNNELS • Display tunnel status or connect to configured tunnel SECURITY POLICY • Display status DYNAMIC DISCOVERY • Display Community of Interest (COI) status
Routes	RIPv2 • Displays RIPv2 Configuration ROUTING TABLE • Displays Red-side Routing Table-Local Enclave Prefix Table

Menu Bar Option	Selectable Tab and Function
Maintenance	ABOUT • Display Device Information PASSWORD • Change Password AUDIT LOG • View Auditable Events • Export Audit Log File

UNCLASSIFIED//FOUO

UNCLASSIFIED//FOUO

Menu Bar Option Button	Function
LOG OFF	Closes Session
REBOOT	• Closes Web Page • Restarts Device • Performs Device Self Test
ZEROIZE	Erases Keys, Login Accounts, and Tunnels

UNCLASSIFIED//FOUO

(U//FOUO) When selecting configuration menu bar options and associated pages, hyperlinks, and option buttons, stopping the page while loading can cause unreliable data to display on the Web page.

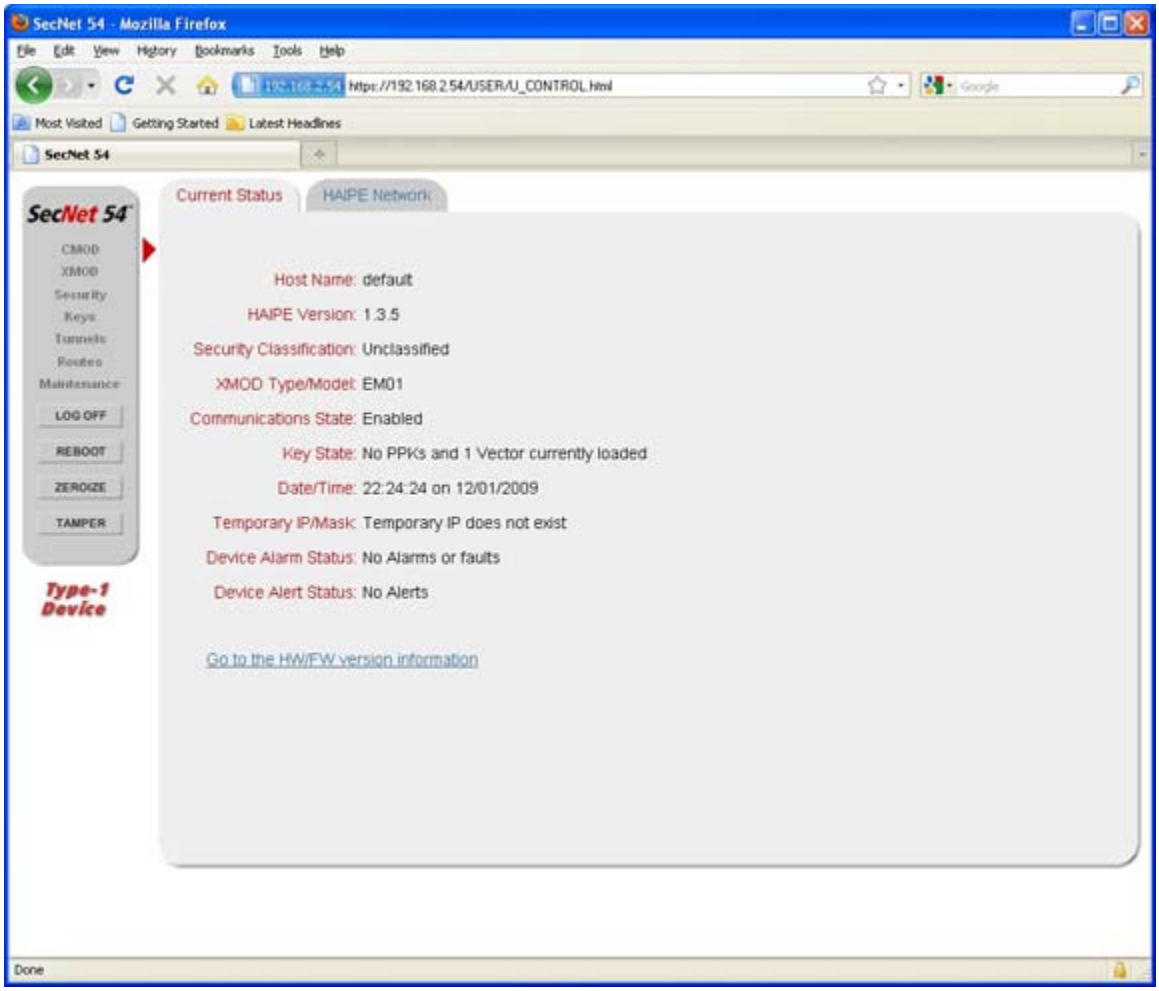
3.2.5 (U) Viewing the KIV-54 Configuration

(U//FOUO) The selected **CMOD (Red)** menu option displays tabs for selecting and displaying KIV-54 cryptographic status. This information is read-only to the User.

3.2.5.1 (U) Viewing the Current Status of the SecNet 54® Device

(U//FOUO) The **Current Status** tab displays the **Current Status** page with the device (Host) Name, the HAIPE® Version, and the Security Classification level as well as the XMOD Model and Communication status, if attached and enabled. This page also indicates the HAIPE® key status, the current date and time (i.e., Greenwich Mean Time (GMT)), and the Temporary IP and Subnet Mask addresses.

UNCLASSIFIED//FOUO



UNCLASSIFIED//FOUO

(U//FOUO) The Alarm Status area (beneath the menu bar) displays device errors and alerts. When the error or alert occurs, selecting the More Info hyperlink in the Alarm Status area causes additional information to display in the Device Alarm Status field and the Device Alert Status field, as appropriate. A Device Alarm Status field displaying “No Alarms or Faults” indicate proper device operation. If the Device Alarm Status field displays a fault code, first cycle power on the KIV-54 and attempt to resume operation of the device. If the fault reoccurs, contact SecNet 54® technical support, and report the displayed fault code. Technical support contact information is provided in Appendix C of this manual.

(U//FOUO) The Device Alert Status field displays the error description and a **Clear Alerts** button as illustrated in the following example.

UNCLASSIFIED//FOUO

UNCLASSIFIED//FOUO

(U//FOUO) The alert is also captured in the device audit log (Section 3.2.11.3) when it meets the audit log's criterion for capture. The alert is not cleared by logging out of the Web pages and displays at each Administrator or User login until cleared. Selecting the **Clear Alerts** button displays the following message while removing the alert description from the **Current Status** page but not from the audit log.

Please wait until your changes are applied...

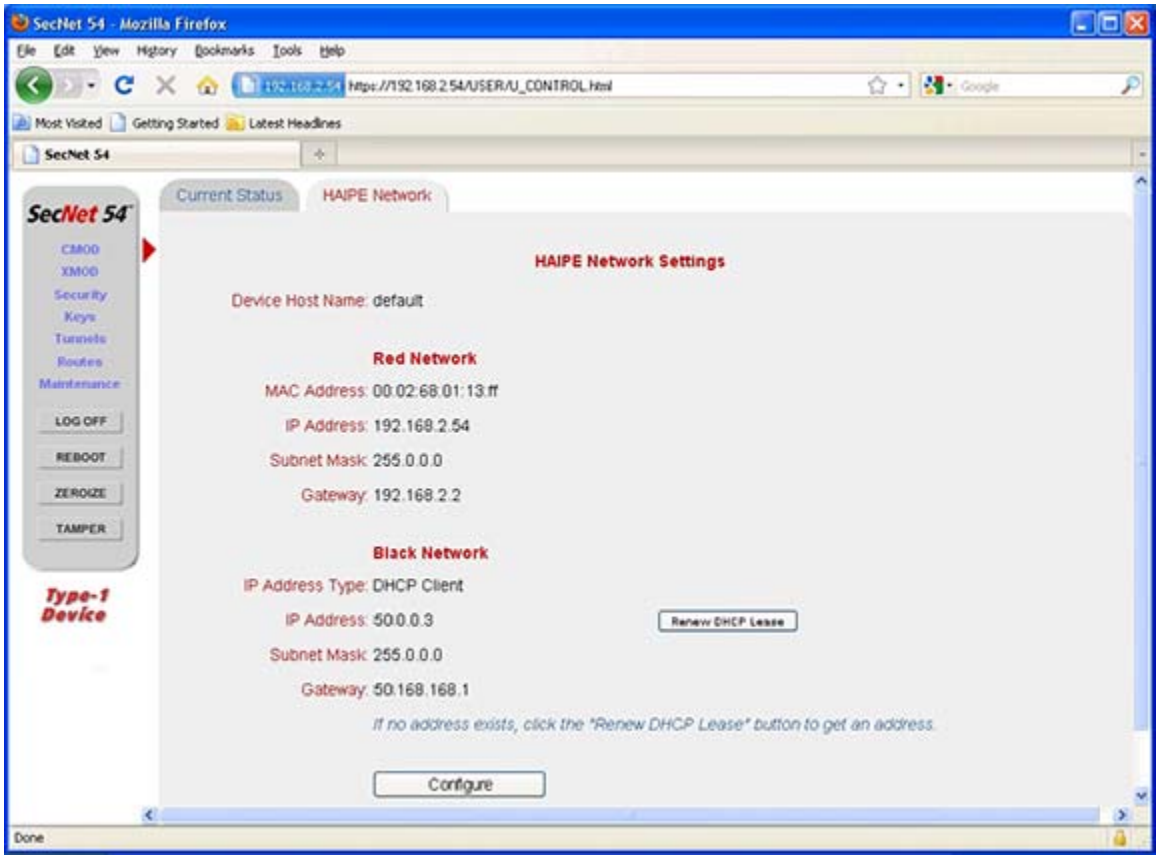
(U//FOUO) Once the alert description is cleared, the **Clear Alerts** button is removed and the Device Alert Status field displays "No Alerts".

(U//FOUO) Selecting the Go to the HW/SW version information hyperlink accesses the **About** status page (Section 3.2.11) of the **Maintenance** menu.

3.2.5.2 (U) Viewing the HAIPE® Network Configuration

(U//FOUO) The **HAIPE Network** tab displays the Device Host Name, the HAIPE® Red (Classified) Network settings, and the HAIPE® Black Network settings. The network settings are view only to the User, but the **Renew DHCP Lease** button is not. However, it is only displayed if the Black Network IP Address Type is configured as a DHCP Client. When configured as Static, the button is removed.

UNCLASSIFIED//FOUO



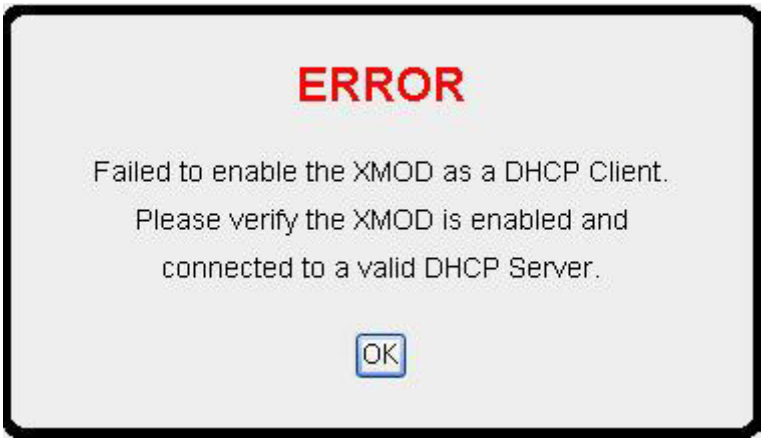
UNCLASSIFIED//FOUO

(U//FOUO) The IP address used with the DHCP Client configuration is leased for a period of time. The DHCP Client can request a lease renewal of the address by the User selecting the **Renew DHCP Lease** button. The DHCP assigned IP address is requested from an external DHCP server. Selecting the **Renew DHCP Lease** button displays the following message:

Please wait while your changes are applied...

(U//FOUO) After saving the change, the **HAIPE Network Settings** page redisplays with the configuration change. Note that selecting the **Renew DHCP Lease** button prior to enabling the XMOD displays the following pop-up message. The **OK** button selection closes the pop-up:

UNCLASSIFIED//FOUO



UNCLASSIFIED//FOUO

3.2.6 (U) Configuring the External Module

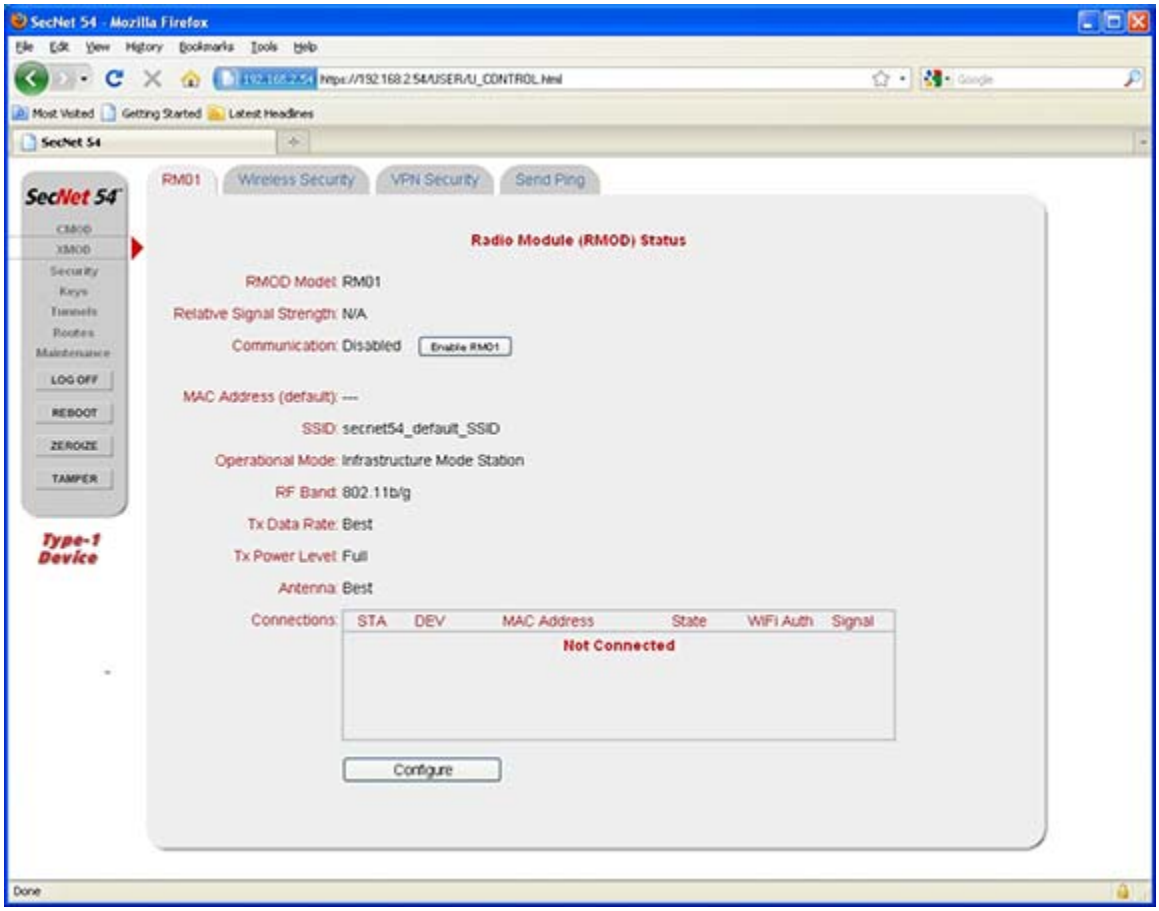
(U//FOUO) The **XMOD** menu option is available with both Administrator and User logins. User privileges associated with this menu option include configuring the RM01, RM01 wireless security settings, and VPN security settings; enabling the RM01 wireless radio; and pinging another device on the Black network.

(U//FOUO) The **RM01** tab page displays the **Radio Module (RMOD) Status** with the configuration of the external module attached to the KIV-54 cryptographic module. The XMOD Model field identifies the type of external module that is attached. If no external module is attached, selecting the **XMOD** menu option displays the following error on the status page.

> *No XMOD is connected.*
>
> *If you have recently connected an XMOD, please refresh the page to view the XMOD status.*

(U//FOUO) RM01 is displayed on the **Radio Module (RMOD) Status** page when the attached external module is an RM01 802.11 wireless radio. The status and configuration items displayed on this page are specific to the RM01. Status and configuration items on the **Radio Module (RMOD) Status** pages for other external module types will be different.

(U//FOUO) The following figure illustrates the **Radio Module (RMOD) Status** page. The settings displayed are sample data; the actual settings will depend on the configuration of the RM01.



(U//FOUO) From the **Radio Module (RMOD) Status** page the User can enable and disable the radio, as well as modify the radio settings (if in the appropriate operating mode). At the bottom of the page, the displayed radio settings include a Connections listing of current SecNet 54® radios associated with this one. If none are associated, a *"Not Connected"* status message is displayed. A scroll bar becomes available when the number of connections exceed the viewing area in the Connections list.

3.2.6.1 (U) Enabling and Disabling the RM01

(U//FOUO) When power is applied to the KIV-54RM01 (SecNet 54® device), the RM01 remains disabled and cannot transmit or receive. The RM01 is disabled until manually enabled with the **Enable RM01** button on the **Radio Module (RMOD) Status** page (refer to Section 3.2.6).

(U//FOUO) When the RM01 Operational Mode is Access Point or Wireless Bridge, the **Enable RM01** button is not displayed to Users. Only an Administrator can Enable or Disable an RM01 that is configured as an Access Point or Wireless Bridge. When the RM01 Operational Mode is Infrastructure Mode Station or Ad Hoc Mode Station, the **Enable RM01** button is available for Users.

NOTE

(U//FOUO) Enabling an Ad Hoc Mode Station may take up to one minute to complete the connection and provide the capability to pass traffic.

(U//FOUO) When the **Enable RM01** is selected, the following status page is displayed.

UNCLASSIFIED//FOUO

UNCLASSIFIED//FOUO

(U//FOUO) The **Radio Module (RMOD) Status** page displays the RM01's stages as communication is enabled. The stages include Enabling RM01, Initializing RM01, and Applying RM01 Settings. As each stage completes, the text changes to green and a check mark appears to the left, as illustrated below.

UNCLASSIFIED//FOUO

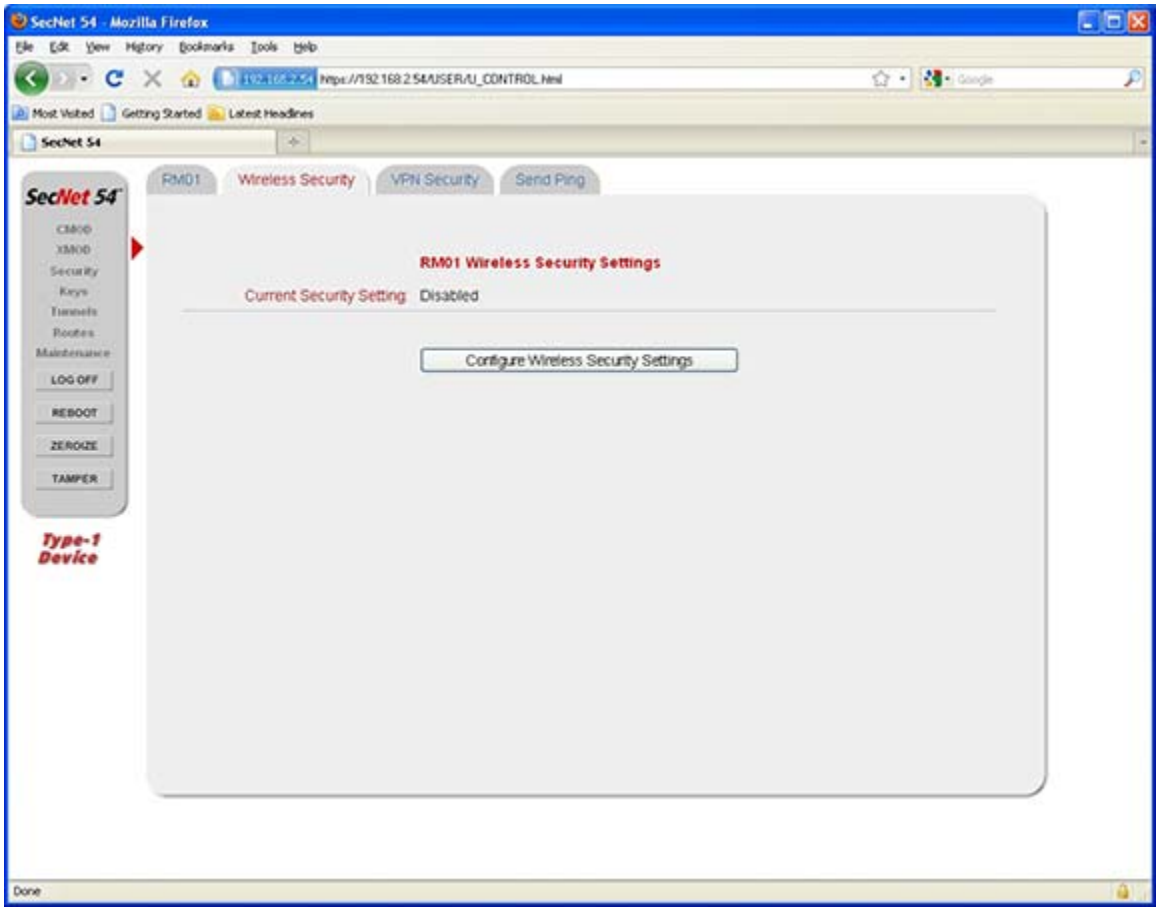
UNCLASSIFIED//FOUO

(U//FOUO) Once the enabling communication process completes, the **Radio Module (RMOD) Status** page re-displays with the **Enable RM01** button name changed to **Disable RM01**. Selecting the **Disable RM01** button terminates communication. The RM01 is then disabled and cannot transmit or receive.

3.2.6.2 (U) Editing the Security Settings

(U//FOUO) Selecting the **Wireless Security** tab displays the **RM01 Wireless Security Settings** page. The following status is displayed when the User or Administrator initially logs into the device prior to editing security settings.

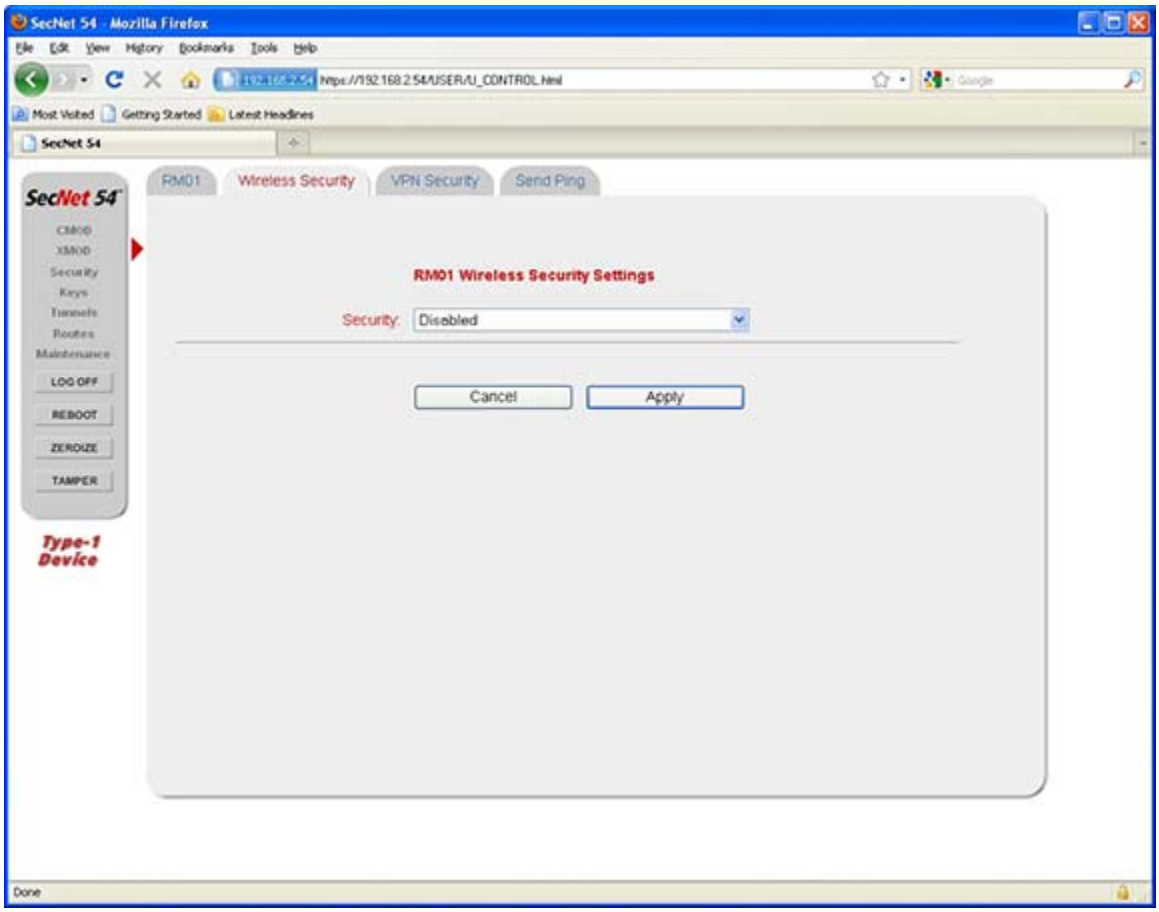
UNCLASSIFIED//FOUO



UNCLASSIFIED//FOUO

(U//FOUO) Selecting the **Configure Wireless Security Settings** button updates the page with a list box containing selectable security settings.

UNCLASSIFIED//FOUO



UNCLASSIFIED//FOUO

(U//FOUO) The following security options are available from the **RM01 Wireless Security Settings** page: Disabled, Wired Equivalent Privacy (WEP), Wi-Fi Protected Access-Pre-Shared Key (WPA-PSK) (Personal) using RC4/TKIP, WPA-PSK (Personal) using AES/CCMP (Legacy), WPA2-PSK (Personal) using AES/CCMP, and WPA2 (Enterprise).

(U//FOUO) Once wireless security settings are configured and saved, the settings are retained when the User logs out of the Web pages, reboots the device, or powers off the device.

(U//FOUO) As a Type-1 encryption device, the KIV-54 does not depend on WEP or WPA security to provide confidentiality. The WEP and WPA settings are provided only for compatibility with commercial equipment. Selecting WEP or WPA security does not enhance or reduce the security of the transmitted data.

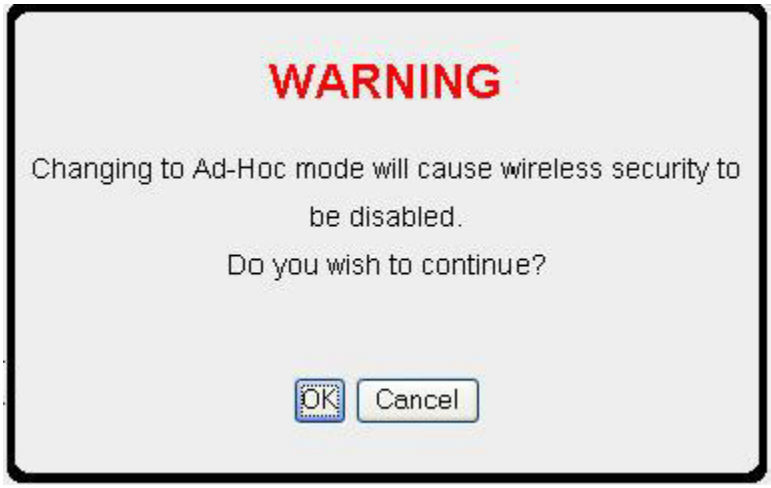
(U//FOUO) RM01 security is modified by a selection of Disabled, WEP, or one of the WPA-PSK or WPA2-PSK personal modes from the Security drop-down list box, but WEP and WPA-PSK are not available for Ad Hoc Station and Wireless Bridge operational modes. If security has been enabled and the operational

mode is changed to Wireless Bridge or Ad Hoc, the following **WARNING** messages are displayed indicating that the wireless security setting cannot be enabled while operating in these modes:

UNCLASSIFIED//FOUO

UNCLASSIFIED//FOUO

UNCLASSIFIED//FOUO



UNCLASSIFIED//FOUO

(U) Selecting the **Cancel** button removes the **WARNING** messages. Selecting the OK button displays the following message:

Please wait until your settings are applied...

(U//FOUO) After the settings are saved, the **Radio Module (RMOD) Status** page displays with the communications disabled.

NOTE

(U//FOUO) If communication is "disabled" when saving WEP and WPA security settings (i.e., selecting the **APPLY** button on the **RM01 Wireless Security Settings** page), the RM01 settings are saved and the following status is displayed on the page:

UNCLASSIFIED//FOUO

UNCLASSIFIED//FOUO

(U//FOUO) If communication is "enabled" when saving WEP and WPA security settings, the RM01 settings are saved and the RM01 radio rebooted as indicated by the following status on the **RM01 Wireless Security Settings** page.

UNCLASSIFIED//FOUO

UNCLASSIFIED//FOUO

(U//FOUO) The following sections describe the WEP and the WPA security settings.

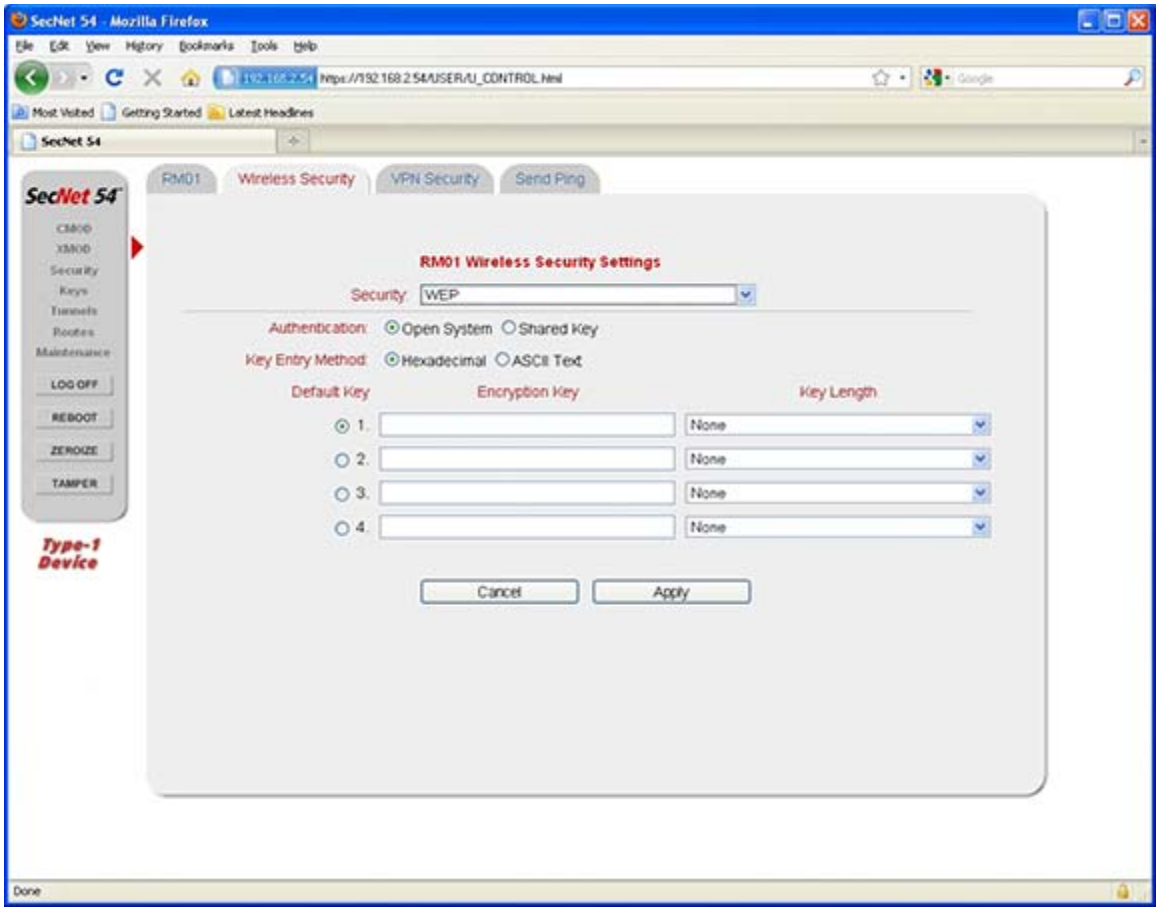
3-2.6.2.1 (U) Setting Wireless Security Parameters for WEP

(U//FOUO) The SecNet 54® RM01 supports the WEP encryption standard for compatibility with commercial equipment that may be using that standard. When WEP is selected from the Security drop-down list box, the **RM01 Wireless Security Settings** page updates and displays configurable fields associated with WEP.

NOTE

(U//FOUO) Users can only change wireless security parameters in Ad Hoc Mode Station or Infrastructure Mode Station.

UNCLASSIFIED//FOUO



UNCLASSIFIED//FOUO

(U//FOUO) The types of authentication and the key entry method are selected from the associated radio buttons. The following is a description of the options:

1. (U//FOUO) Authentication

   - (U) Open System - allows any device, regardless of WEP keys, to authenticate and attempt to associate.
   - (U) Shared Key - indicates to the Access Point to send a plain text, shared key query to any device that attempts to associate with the Access Point.

2. (U//FOUO) Key Entry Method

    - (U) Hexadecimal - A base-16 number system that consists of 16 unique symbols, 0 to 9 and A to F.
    - (U) ASCII Text - A code for representing English characters as numbers, with each letter assigned a number from 0 to 127.

3. (U//FOUO) Default Key - allows the User to enter WEP keys in either of the following lengths and formats:
    - (U) Ten (10) hexadecimal digits or 5 ASCII characters for 40-bit WEP keys
    - (U) Twenty-six (26) hexadecimal digits or 13 ASCII characters for 104-bit WEP keys
    - (U) The Default Key Length selection is None

(U//FOUO) The following special characters are not valid WEP Key values: double quotes, single quote, less than, greater than, and ampersand.

(U//FOUO) When editing WEP wireless security settings, the **Cancel** button selection rescinds the selections and redisplays the **RM01 Wireless Security Settings** status page with previous security settings intact. The **Apply** button selection initiates the verification process and displays status based on whether the device's communication is enabled or disabled (as illustrated in Section 3.2.6.2). Once the process completes, the new WEP security settings are displayed.

3-2.6.2.2 (U) Setting Wireless Security Parameters for WPA-PSK (Personal)

(U//FOUO) When the Security drop-down arrow is selected on the **RM01 Wireless Security Settings** page, the following WPA Personal security modes are displayed in the drop-down list box.

- (U//FOUO) WPA-PSK (Personal) using RC4/TKIP
- (U//FOUO) WPA-PSK (Personal) using AES/CCMP (Legacy)
- (U//FOUO) WPA2-PSK (Personal) using AES/CCMP

(U//FOUO) WPA-PSK and WPA2-PSK operate in an unmanaged mode and use a Pre-shared Key (PSK) for authentication. This mode requires manually entering a pass phrase (the PSK) on the Access Point to generate the encryption key. The Pass Phrase key entry method is either hexadecimal or ASCII. The encryption method for WPA is Temporal Key Integrity Protocol (TKIP) or Counter-Mode/CBC-MAC Protocol (CCMP) called the Advanced Standard (AES) and for WPA2 it is the CCMP called the AES.

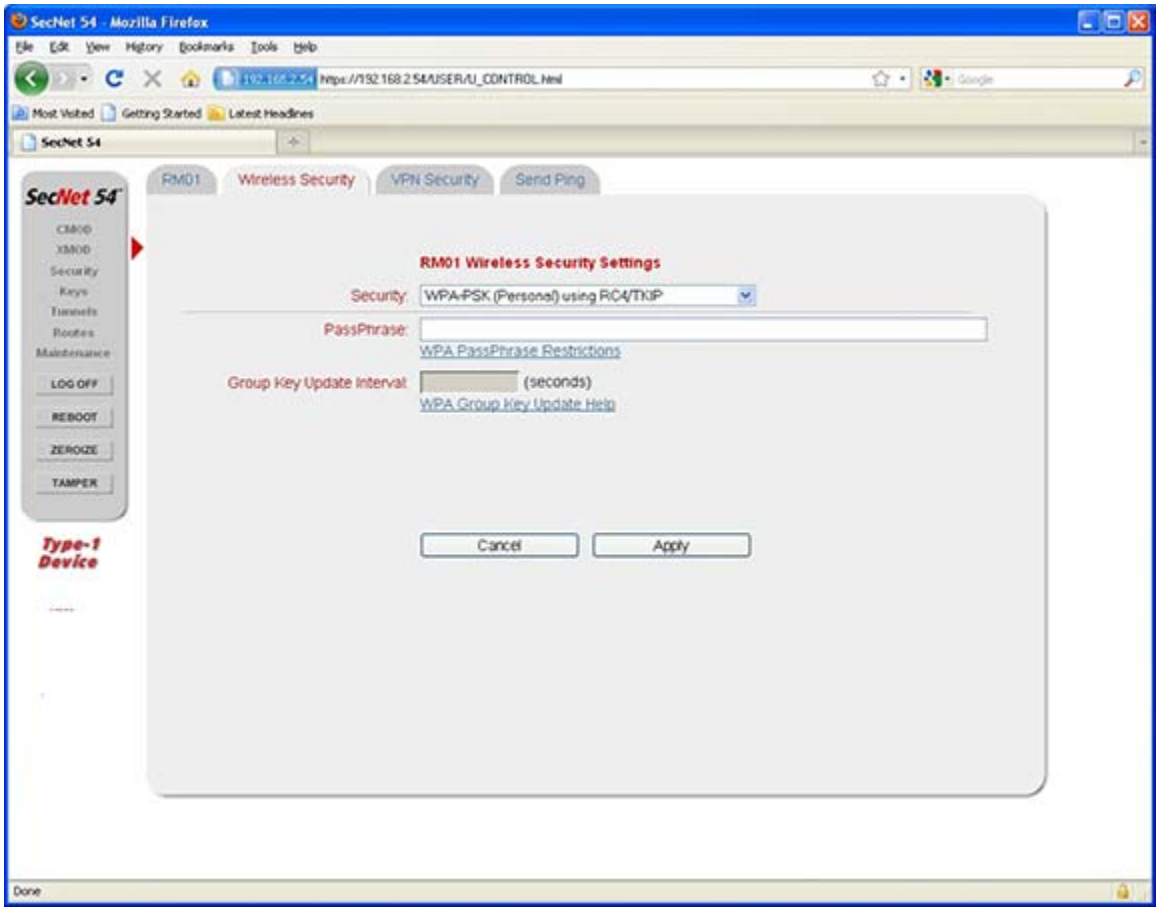
(U//FOUO) WPA-PSK (Personal) using AES/CCMP (Legacy) is only selected when communicating with previous releases of the SecNet 54® software in the WPA-PSK mode using the Cipher Suite AES/CCMP.

(U//FOUO) The Group Key Update Interval data field is only available if the SecNet 54® device is in the Access Point operational mode. The figure below illustrates **RM01 Wireless Security Settings** configuration page with WPA-PSK (Personal) using RC4/TKIP selected.

NOTE

(U//FOUO) Users can only change wireless security parameters in Infrastructure Mode Station.

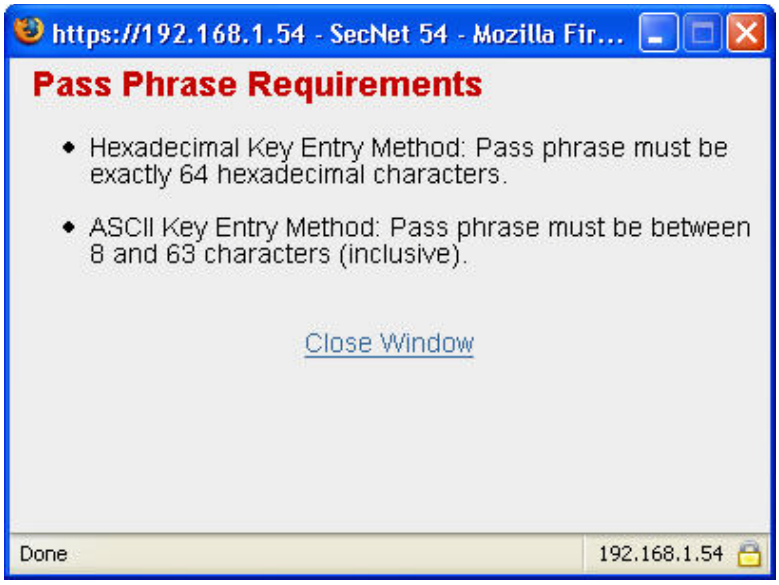
UNCLASSIFIED//FOUO



UNCLASSIFIED//FOUO

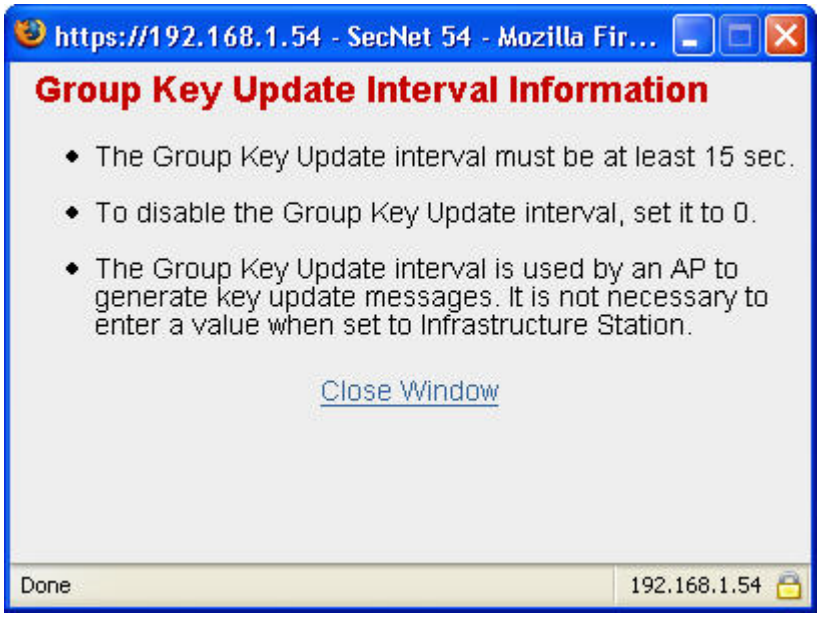
(U//FOUO) The **RM01 Wireless Security Settings** page contains links to information about criteria for entering WPA data. The **WPA PassPhrase Restrictions** and the **WPA Group Key Update Help** selections display requirements in Web browser windows for Pass Phrase and Group Key Updates.

UNCLASSIFIED//FOUO



UNCLASSIFIED//FOUO

UNCLASSIFIED//FOUO



UNCLASSIFIED//FOUO

(U//FOUO) The following special characters are not valid Pass Phrase values: double quotes, single quote, less than, greater than, and ampersand. Entering incorrect information into the PassPhrase data entry field displays an error message.

(U//FOUO) The following figure is an example of a Pass Phrase error message:

UNCLASSIFIED//FOUO

UNCLASSIFIED//FOUO

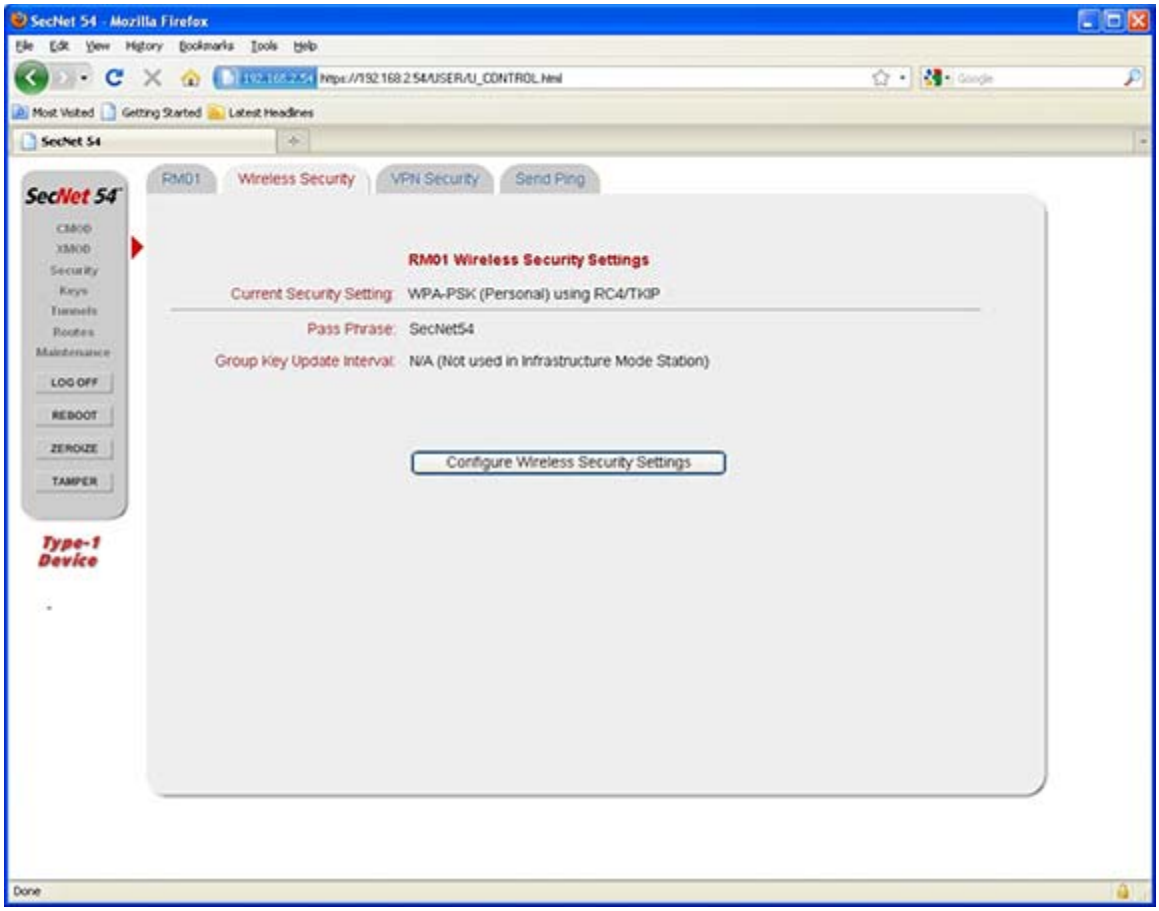
(U//FOUO) Entering incorrect information into the Group Key Update Interval data entry field also displays an error message. The following figure is an example of a Group Key Update Interval error message.

UNCLASSIFIED//FOUO

UNCLASSIFIED//FOUO

(U//FOUO) The WPA-PSK and WPA2-PSK security settings are modified with the RM01 enabled or disabled. Selecting the **Cancel** button negates the new security selection and the previous setting remains. The **Apply** button selection initiates the verification process and displays status based on whether the device's communication is enabled or disabled (as illustrated in Section 3.2.6.2). Once this process completes, the new WPA security setting is displayed on the **RM01 Wireless Security Settings** status page.

UNCLASSIFIED//FOUO



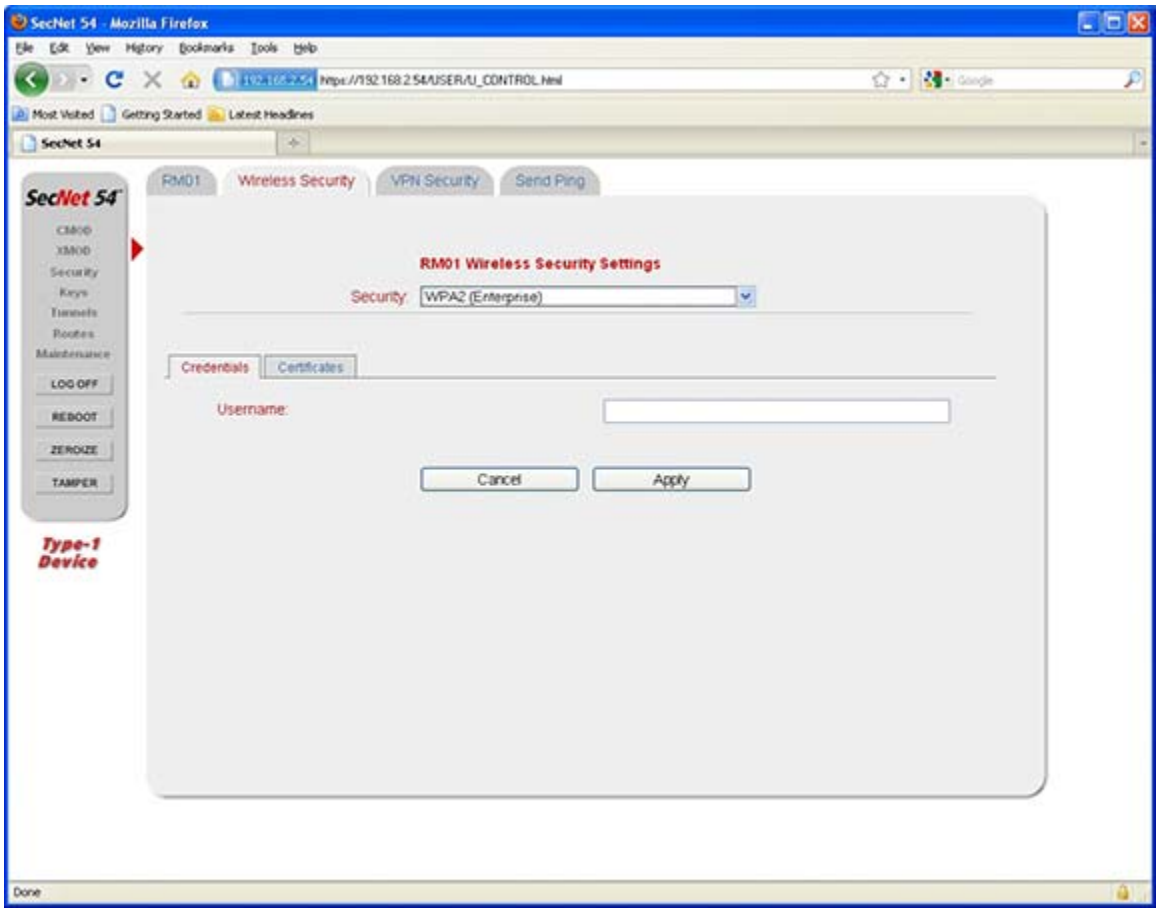
UNCLASSIFIED//FOUO

3-2.6.2.3 (U) Setting Wireless Security Parameters for WPA2 (Enterprise)

(U//FOUO) The RM01 radio also supports WPA2 in the Enterprise mode. WPA2 (Enterprise) operates in a managed mode and uses an Extensible Authentication Protocol (EAP) type with an authentication server to provide mutual authentication between the Client and authentication Server via the access point. In Enterprise mode a unique key mechanism is assigned for access to the WLAN. It uses AES encryption type.

(U//FOUO) WPA2 (Enterprise) is only available in the Infrastructure operational mode. When WPA2 (Enterprise) is selected from the Security drop-down list box on the **RM01 Wireless Security Settings** page, two tabs are displayed, **Credentials** and **Certificates**. The security certificates and key pairs are not provided by Harris Corporation. They are developed and used by the customer for authentication when using WPA2 (Enterprise). The certificates and key pairs are loaded through the **CMOD Security** menu (refer to Section 3.2.7.3). Note that the CA Certificates and Public/Private Key Pairs called out and illustrated in this section are examples only.

UNCLASSIFIED//FOUO

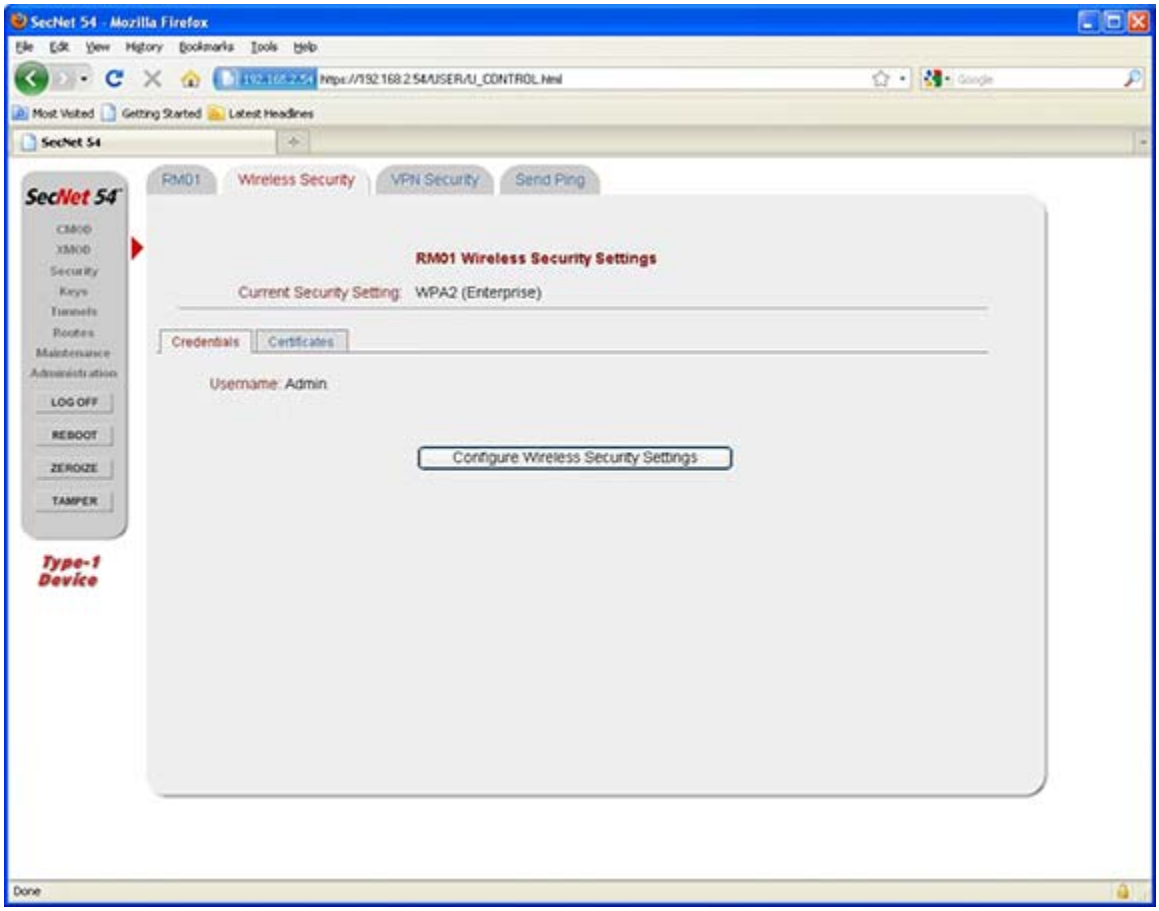


UNCLASSIFIED//FOUO

(U//FOUO) The **Credentials** tab selection allows the use of a username but it may or may not be required. The requirement of a username depends on the RADIUS Authentication server.

(U//FOUO) Selecting the **Cancel** button before or after entering a Username removes the page and displays the previous page with the security setting unchanged. If a Username is entered, selecting the **Apply** button saves the name and the page is updated as illustrated in the following example.

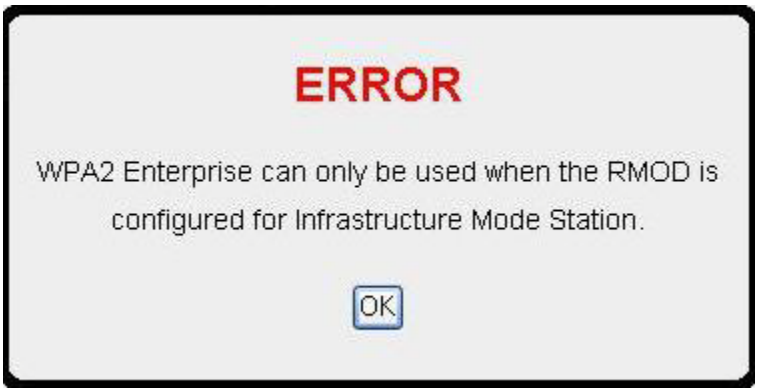
UNCLASSIFIED//FOUO



UNCLASSIFIED//FOUO

(U//FOUO) However, if the **Apply** button is selected and the RM01 radio is not in the infrastructure operational mode, the following message displays:

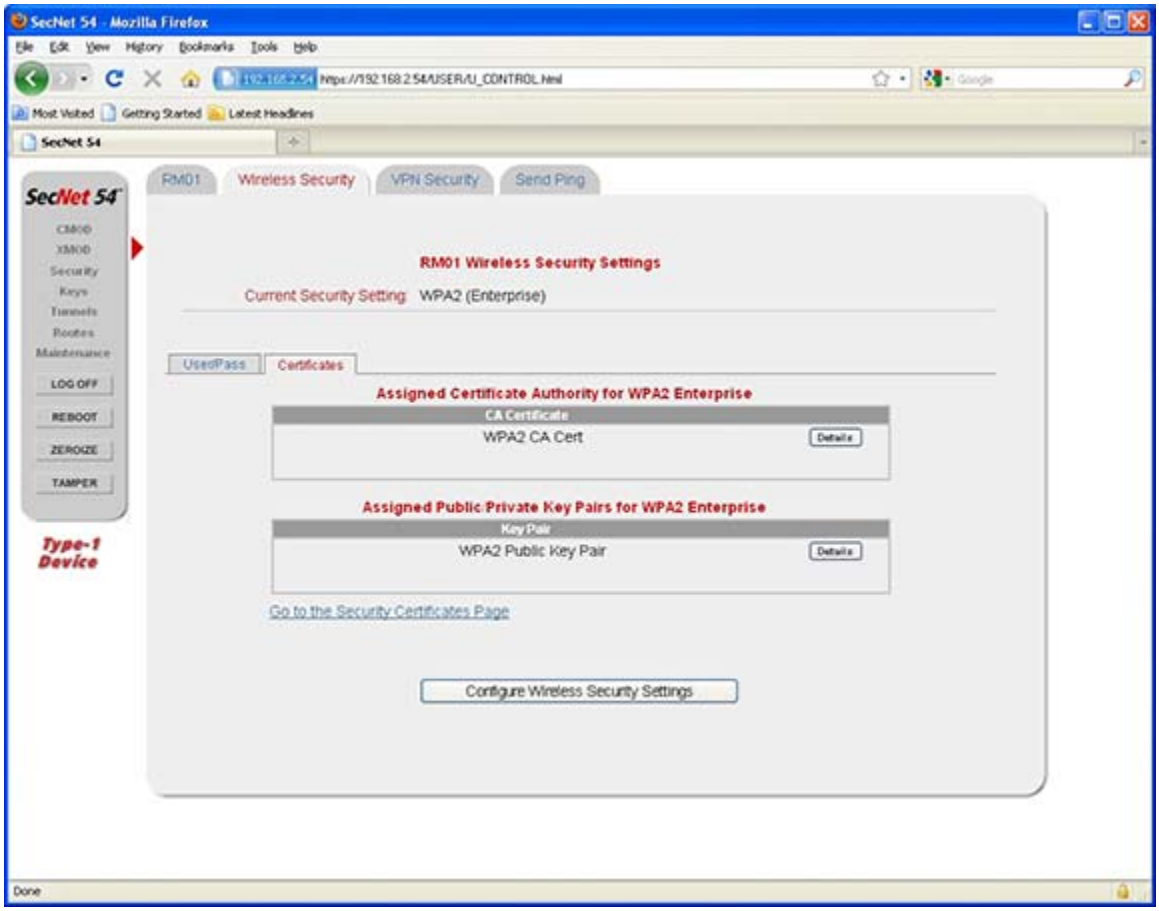
UNCLASSIFIED//FOUO



UNCLASSIFIED//FOUO

(U//FOUO) Selecting the **Certificates** tab displays the Security CA Certificates and Public/Private Key Pairs that have been loaded through the **Security** menu.

UNCLASSIFIED//FOUO



UNCLASSIFIED//FOUO

(U//FOUO) Selecting the Go to the certificate page hyperlink accesses the **Security** menu option to load the WPA2 CA Certificate and WPA2 Public/Private Key Pair (i.e., Client Certificate), if necessary. Selecting the **Details** button associated with the CA certificate and Public/Private Key Pair displays the **Security Details** window for each certificate illustrated in the following examples.

UNCLASSIFIED//FOUO

UNCLASSIFIED//FOUO

UNCLASSIFIED//FOUO

UNCLASSIFIED//FOUO

(U) Each window contains a scroll bar and displays a description of the certificate, including data such as the version number, serial number, and issuer. Selecting the **OK** button, located at the bottom of the window, closes the window.

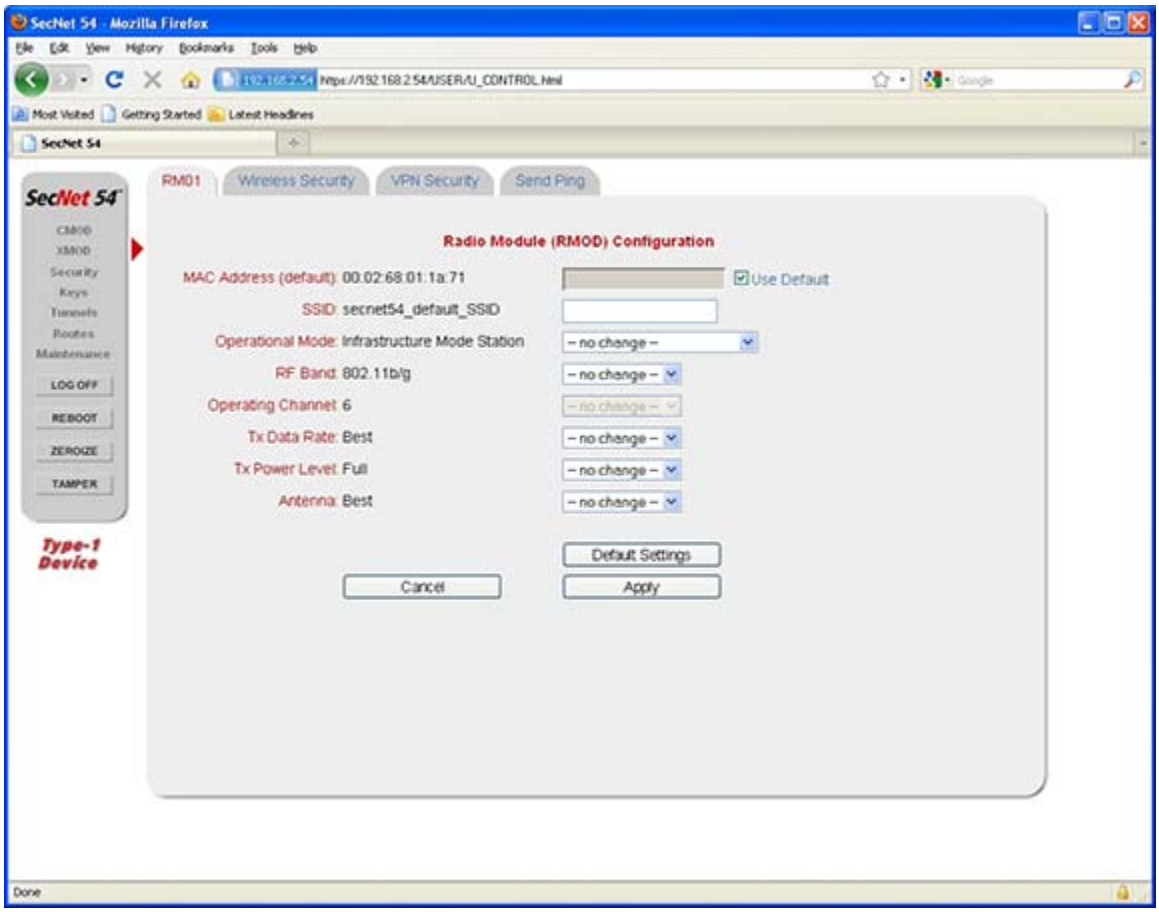
3-2.6.2.4 (U) Disabling the Security Settings

(U//FOUO) The RM01 security setting is disabled from the **RM01 Wireless Security Settings** page. When Disabled is selected from the Security drop-down list box and the **Apply** button is selected, the **RM01 Wireless Security Settings** page displays status based on whether the device's communication is enabled or disabled (as illustrated in Section 3.2.6.2). After saving the setting, the **RM01 Wireless Security Settings** status page displays with the current security setting disabled as illustrated in Section 3.2.6.2.

3.2.6.3 (U) Modifying RM01 Settings

(U//FOUO) Selecting the **Configure** button, which is located on the **Radio Module (RMOD) Status** page, displays the **Radio Module (RMOD) Configuration** page as illustrated in the following figure.

UNCLASSIFIED//FOUO



UNCLASSIFIED//FOUO

(U//FOUO) The **Radio Module (RMOD) Configuration** page displays configurable radio values with associated data entry fields. The MAC Address field is used to enter a MAC address that temporarily overrides the default MAC address. The MAC address is used to “clone” the MAC address of another device on the network. However, if the “Use Default” checkbox is selected, the default MAC address is used. The MAC Address text indicates if the default is being used or if the address is being cloned by displaying “default” or “clone” as appropriate in the parenthesis beside the text. Refer to the following figure.

UNCLASSIFIED//FOUO

UNCLASSIFIED//FOUO

(U//FOUO) On the configuration page the boxes with the drop-down arrows offer a list of choices; the default choice is “no change.” While an Administrator can change all RM01 configurable values, a User can only change RM01 values of an Ad Hoc Mode Station or Infrastructure Mode Station. A User cannot change the configuration of an Access Point or Wireless Bridge. Nor can a User change an Ad Hoc Mode Station or Infrastructure Mode Station to an Access Point or Wireless Bridge.

(U//FOUO) The following special characters are not valid SSID values: double quotes, single quote, less than, greater than and ampersand. Also, the variables in the Operating Channel drop-down list box change based on the frequency selected for RF Band. The listing is unavailable when the device is in the Infrastructure Mode Station because the device searches all changes in the selected band for the defined SSID.

(U//FOUO) The **Cancel** button selection negates any entered changes and returns to the **Radio Module (RMOD) Status** page without changing the RM01 radio configuration. The **Default Settings** button populates the data entry fields with default values. When the **Apply** button is selected, the following message is displayed:

Please wait while your changes are applied...

(U//FOUO) After the message clears, the **Radio Module (RMOD) Status** page is updated with a visual indication of the save process. Status indicators are based on whether the device’s communication is enabled or disabled (as illustrated in Section 3.2.6.2).

(U//FOUO) The save process includes saving the settings and reconfiguring the RM01 radio. Once the process completes, the **Radio Module (RMOD) Status** page redisplays with the RM01’s new property values.

3.2.6.4 (U) Configuring RM01 Virtual Private Networking (VPN) Security Parameters

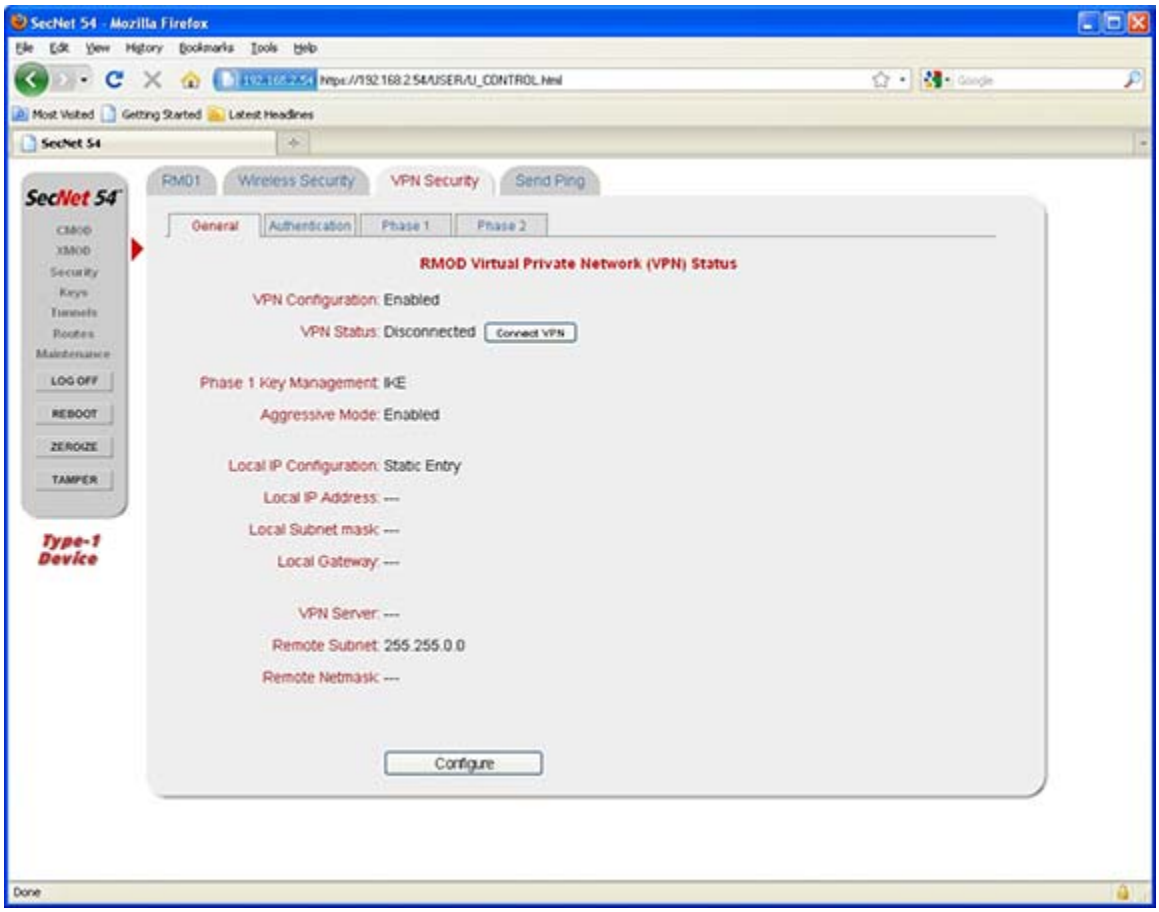
(U//FOUO) The RM01 supports commercial VPN IP Security (IPSec) standards to enable the SecNet 54® device to interoperate with commercial equipment. Any confidentiality, authentication, or data integrity provided by commercial VPN is in addition to that provided by HAIPE®. To interoperate with existing commercial-standard VPNs, it is necessary for the RM01 to be configured to match the settings of the existing host network. Therefore, the VPN settings of the RM01 are similar to those of any commercial device with VPN capability.

(U//FOUO) An Administrator can configure VPN security parameters and enable VPN tunnels. A User can configure VPN tunnels but can only enable them if the device is in the Infrastructure Station or Ad Hoc Station operational modes.

(U//FOUO) When establishing a VPN tunnel, Internet Key Exchange (IKE) requires two phases, Phase 1 and Phase 2. Phase 1 establishes the Internet Security Association Key Management Protocol (ISAKMP) tunnel that manages one or more Phase 2 IPSec data tunnels. Phase 1 involves confirmation among nodes that are about to establish a secure connection across an unsecure network. This process is to verify that each node is authorized to establish this type of connection. When Phase 1 setup is complete, then Phase 2 setup configuration is completed, which involves traffic management of the data communication between nodes.

(U//FOUO) VPN Security parameters are accessible by selecting the **VPN Security** tab and four additional tab pages, **General**, **Authentication**, **Phase 1**, and **Phase 2** as illustrated. Each of these status and configuration pages are described in the following sections.

UNCLASSIFIED//FOUO

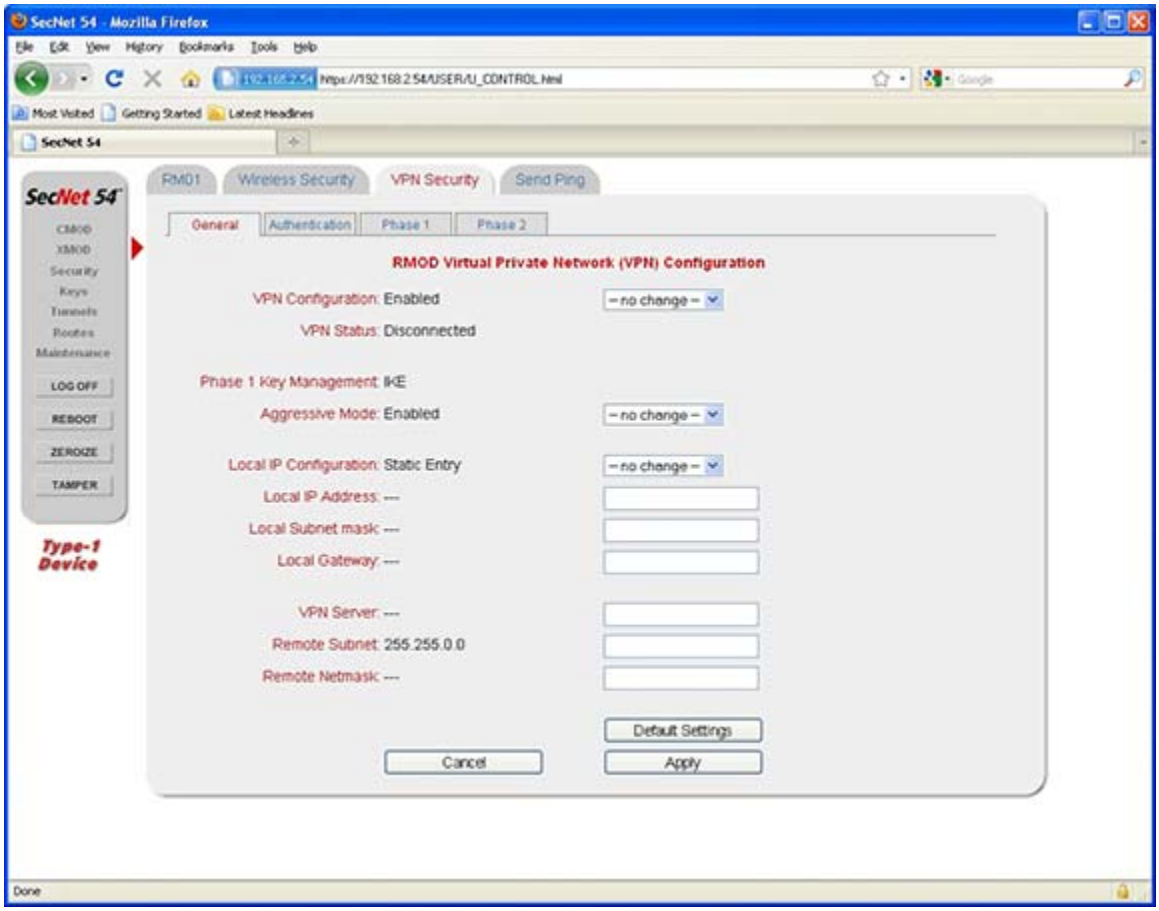


UNCLASSIFIED//FOUO

(U//FOUO) To establish VPN security the following conditions must be met: RM01 communications enabled, VPN keys loaded, and configuration completed by entering or selecting values on all four VPN security configuration pages.

3-2.6.4.1 (U) Setting RM01 VPN Parameters

(U//FOUO) The **General** tab displays the **RMOD Virtual Private Network (VPN) Status** page (refer to Section 3.2.6.4). The **Configure** button selection displays the **RMOD Virtual Private Network (VPN) Configuration** page.



(U//FOUO) The non-editable VPN Status field indicates if a VPN tunnel is connected or disconnected and the VPN tunnel can be enabled or disabled by selecting Enabled or Disabled from the VPN Configuration drop-down list box. Enabling VPN configures the local address on the Black network. VPN is connected to (U//FOUO) establish an IPSec session between the RM01 and the remote VPN server.

(U//FOUO) The Phase 1 Key Management field indicates the VPN tunnel key type. The IPSec VPN supports two types of key-obtained methods, manual key and IKE. The manual key approach indicates that two endpoint VPN gateways require setting up authentication and encryption key by the Administrator manually. The IKE approach performs automatic Internet key exchange. Administrators at both endpoint gateways only need to set the same preshared key.

(U//FOUO) Additional fields are listed and described below:

- (U//FOUO) Aggressive Mode - This mode is either Enabled or Disabled. Enabling this mode accelerates establishing a tunnel.
- (U//FOUO) Local IP Configuration - Static or DHCP Client is selected from the drop-down list box.

- (U//FOUO) The Static selection populates the Local network fields with default network addresses or fields are manually entered.

- (U//FOUO) The DHCP Client selection automates the assignment of the Local IP Address, Local Subnet Mask, and the Local Gateway from the DHCP server.

- (U//FOUO) Local IP Address - The local IP address on the Black network.
- (U//FOUO) Local Subnet Mask - The Subnet Mask of the network where the local IP address resides.
- (U//FOUO) Local Gateway - The address of the Gateway on the local network.
- (U//FOUO) Remote Gateway - IP address of the remote VPN gateway.
- (U//FOUO) Remote Subnet - The subnet of the remote VPN gateway's local network. It can be a host, a partial subnet, or a whole subnet.
- (U//FOUO) Remote Netmask - The Subnet Mask of the remote network.

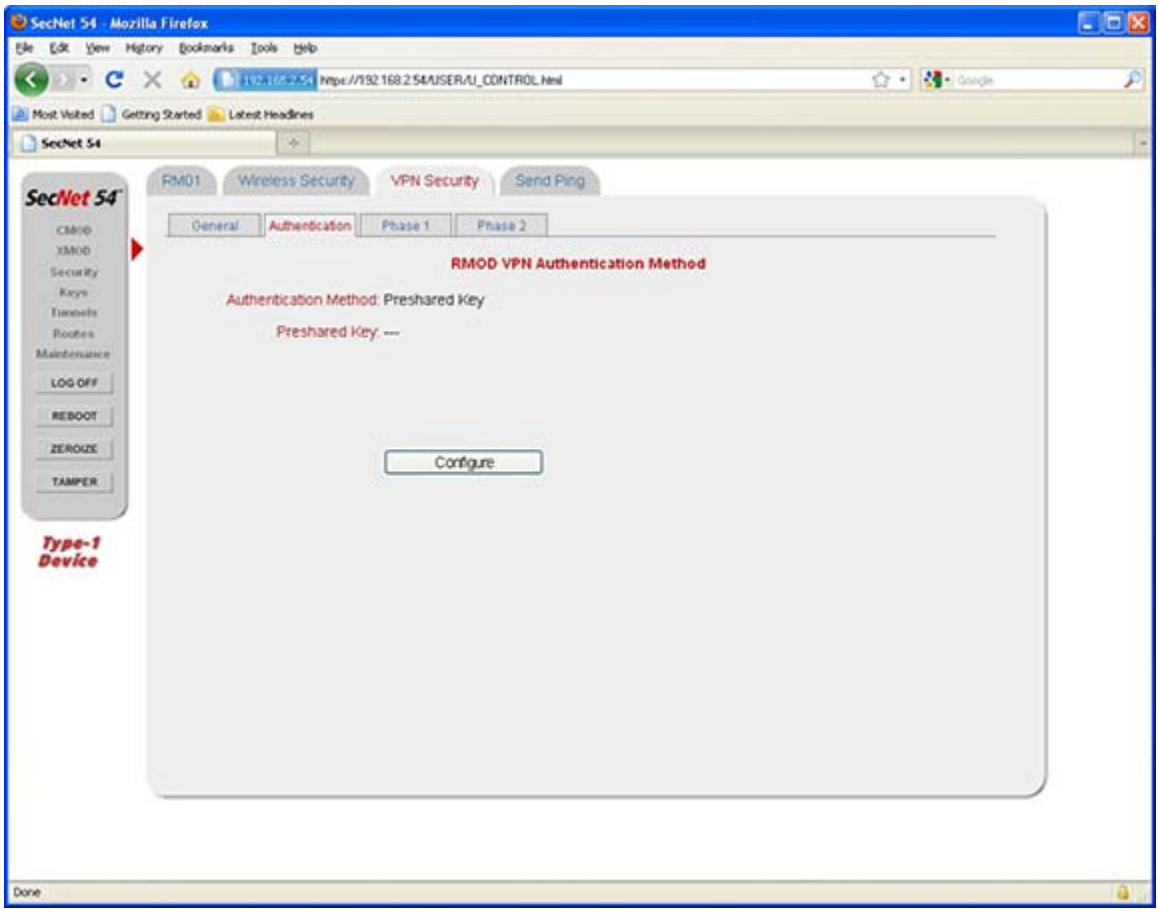
(U//FOUO) The **Cancel** button selection redisplays the status page without saving the modifications, and the **Default Settings** button selection disables the data entry fields for selection. Selecting the **Apply** button, briefly displays the following message and saves the modified values or the default settings:

Please wait while your changes are applied...

3-2.6.4.2 (U) Setting RM01 VPN Authentication Method Parameters

(U//FOUO) The **Authentication** tab displays the **RMOD VPN Authentication Method** status.

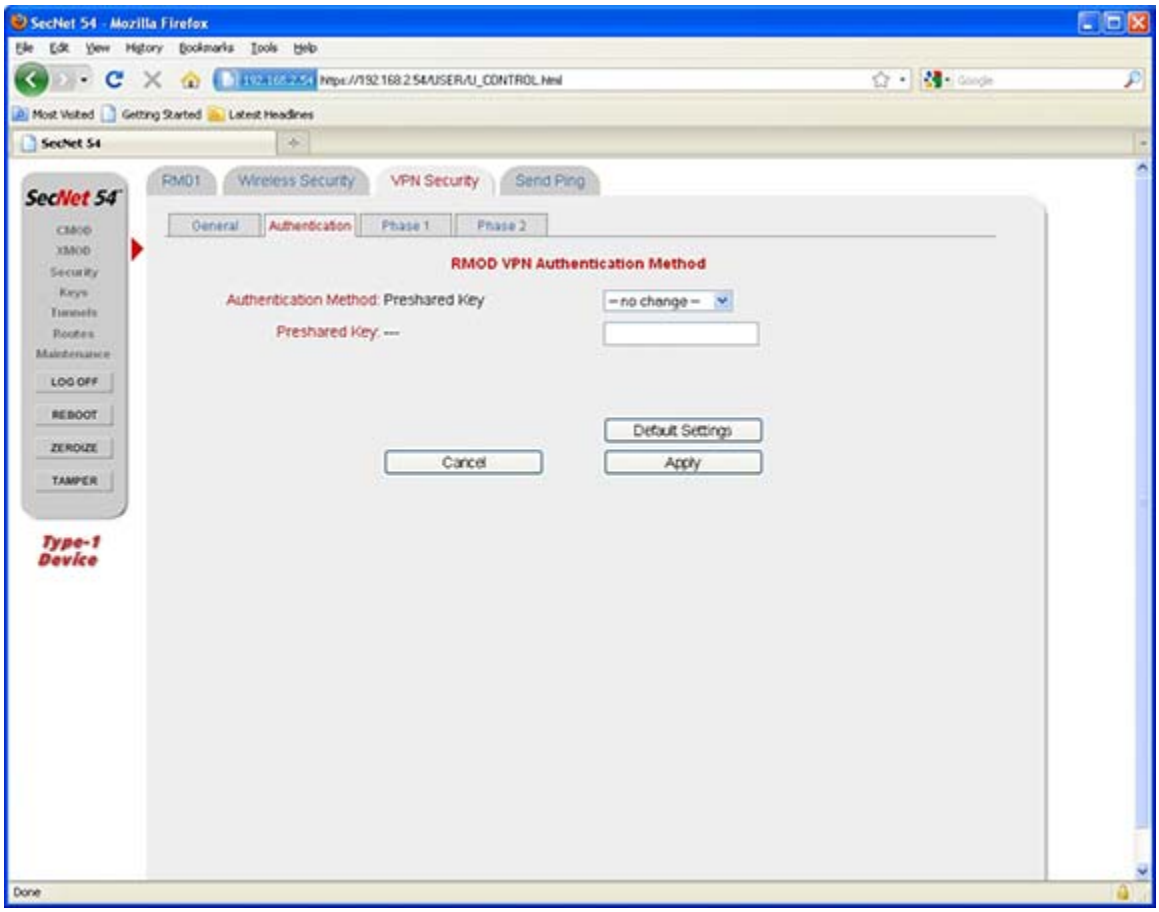
UNCLASSIFED//FOUO



UNCLASSIFIED//FOUO

(U//FOUO) Selecting the **Configure** button displays the **RMOD VPN Authentication Method** configuration page with modifiable data entry fields.

UNCLASSIFIED//FOUO

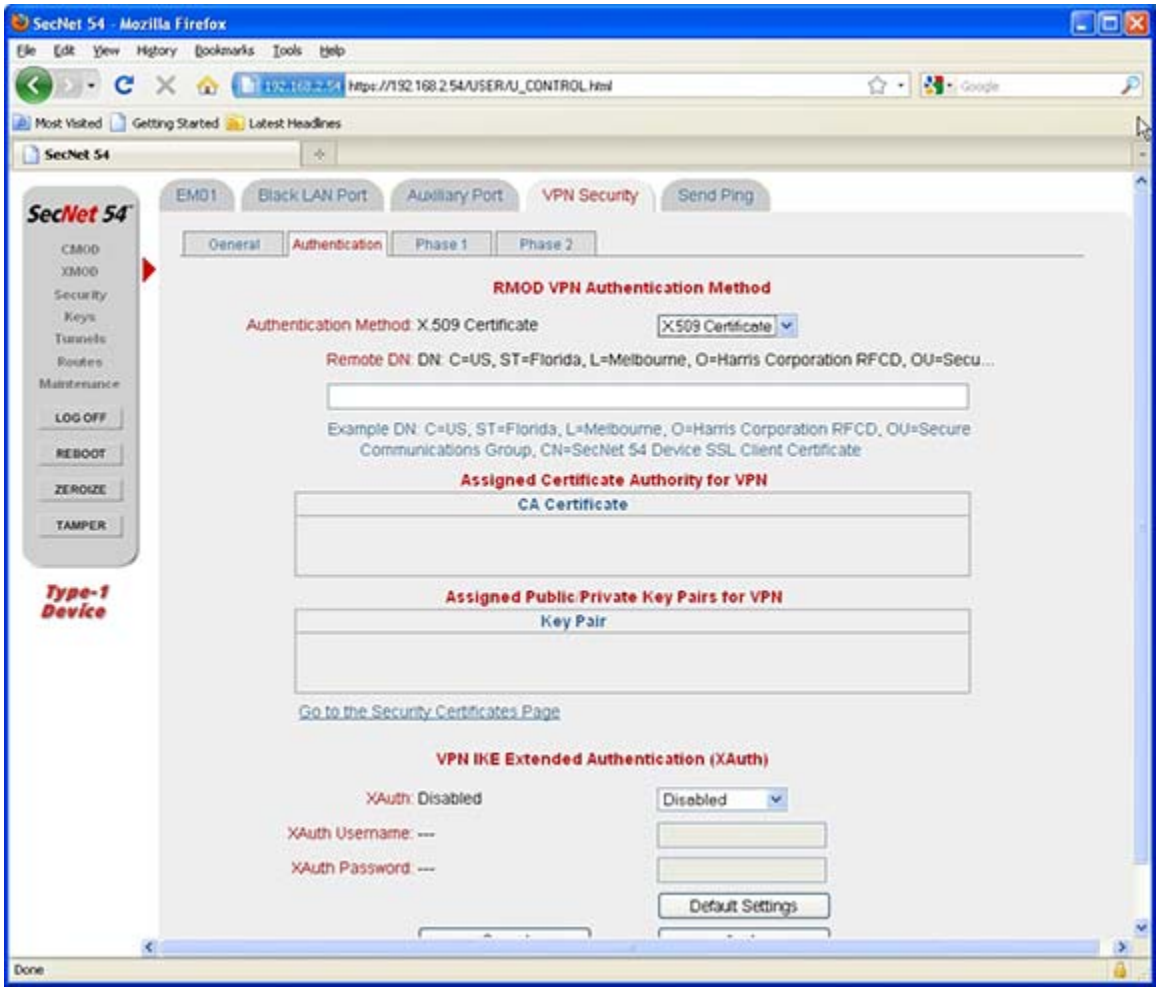


UNCLASSIFIED//FOUO

(U//FOUO) The drop-down list box associated with the Authentication Method displays three key types for selection, Preshared Key, Group, and X509 Certificate. Selecting the Preshared Key requires entering a Preshared Key password in the associated data entry field. The Preshared Key is the first key that supports IKE mechanism of both VPN gateways for negotiating further security keys. The Preshared Key must be the same for both endpoint gateways. Selecting the Group option requires entering a Group Name and a Group Password in the associated data entry fields.

(U//FOUO) Selecting X509 Certificate updates the page with the following two tables: Assigned Certificate Authority for VPN and Assigned Public/Private Key Pairs for VPN.

UNCLASSIFIED//FOUO



UNCLASSIFIED//FOUO

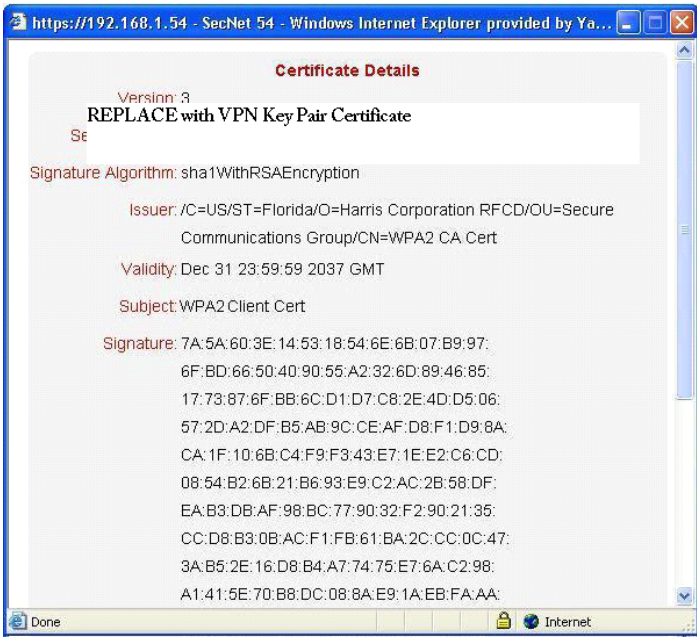
(U//FOUO) If VPN Certificates have been loaded via the **Security** menu option, the Assigned Certificate Authority table contains the CA Certificate and the Assigned Key Pairs table contains the Client Certificate. The CA Certificate and Key Pair are not provided by Harris® Corporation. They are developed and used by the customer for VPN authentication.

(U//FOUO) Selecting the **Details** button associated with each certificate displays the **Details** window for each certificate as illustrated in the following figures.

UNCLASSIFIED//FOUO

UNCLASSIFIED//FOUO

UNCLASSIFIED//FOUO



UNCLASSIFIED//FOUO

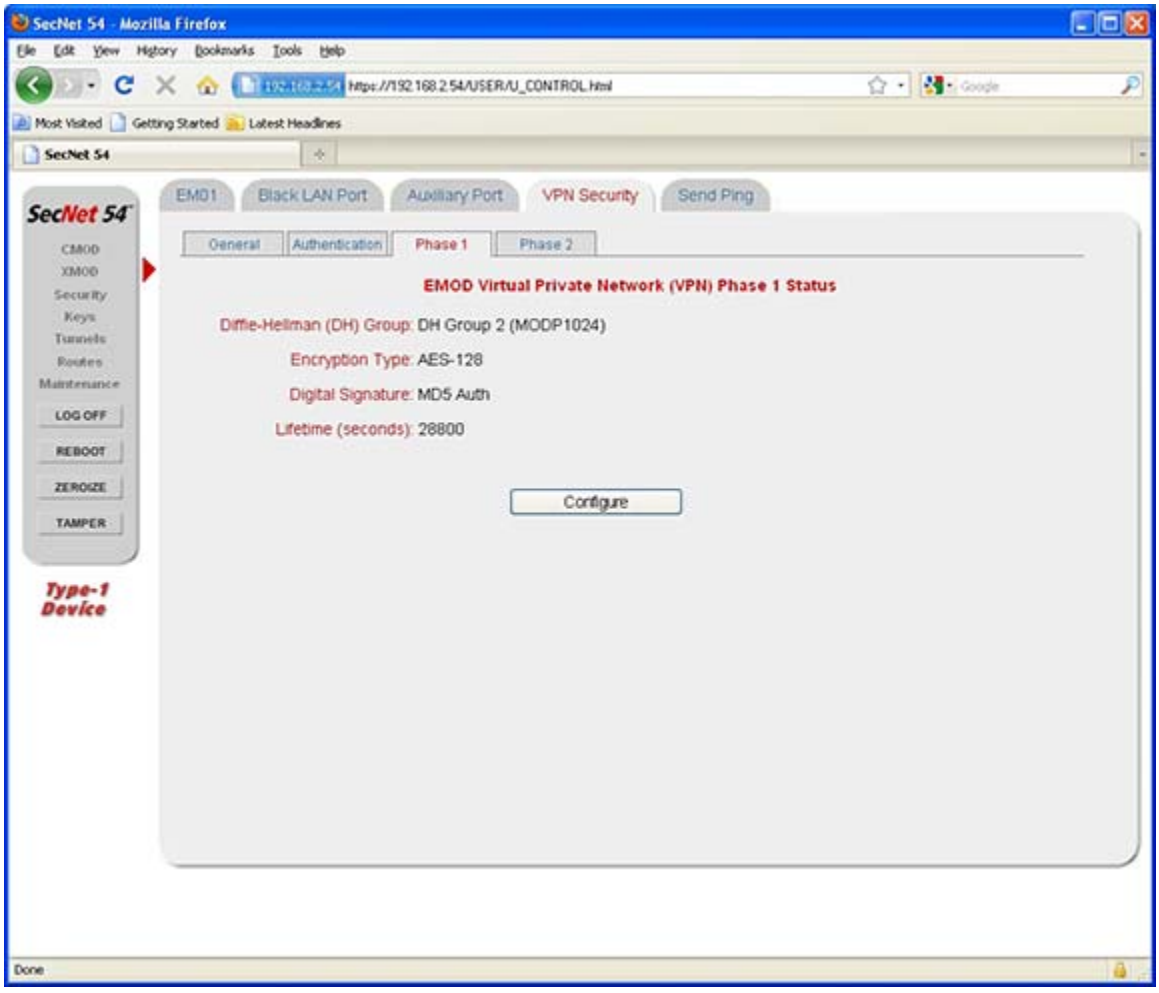
(U//FOUO) When an Authentication Method is selected from the **RMOD VPN Authentication Method** page, selecting the **Cancel** button selection redisplays the status page without saving the modifications. The **Default** button selection populates the data entry fields with the default settings. Selecting the **Apply** button displays the following status message and saves the modified values or default settings, as applicable:

Please wait while your changes are being applied...

3-2.6.4.3 (U) Setting RM01 VPN Phase 1 Parameters

(U//FOUO) The **Phase 1** tab displays the **RMOD Virtual Private Network (VPN) Phase 1 Status** page.

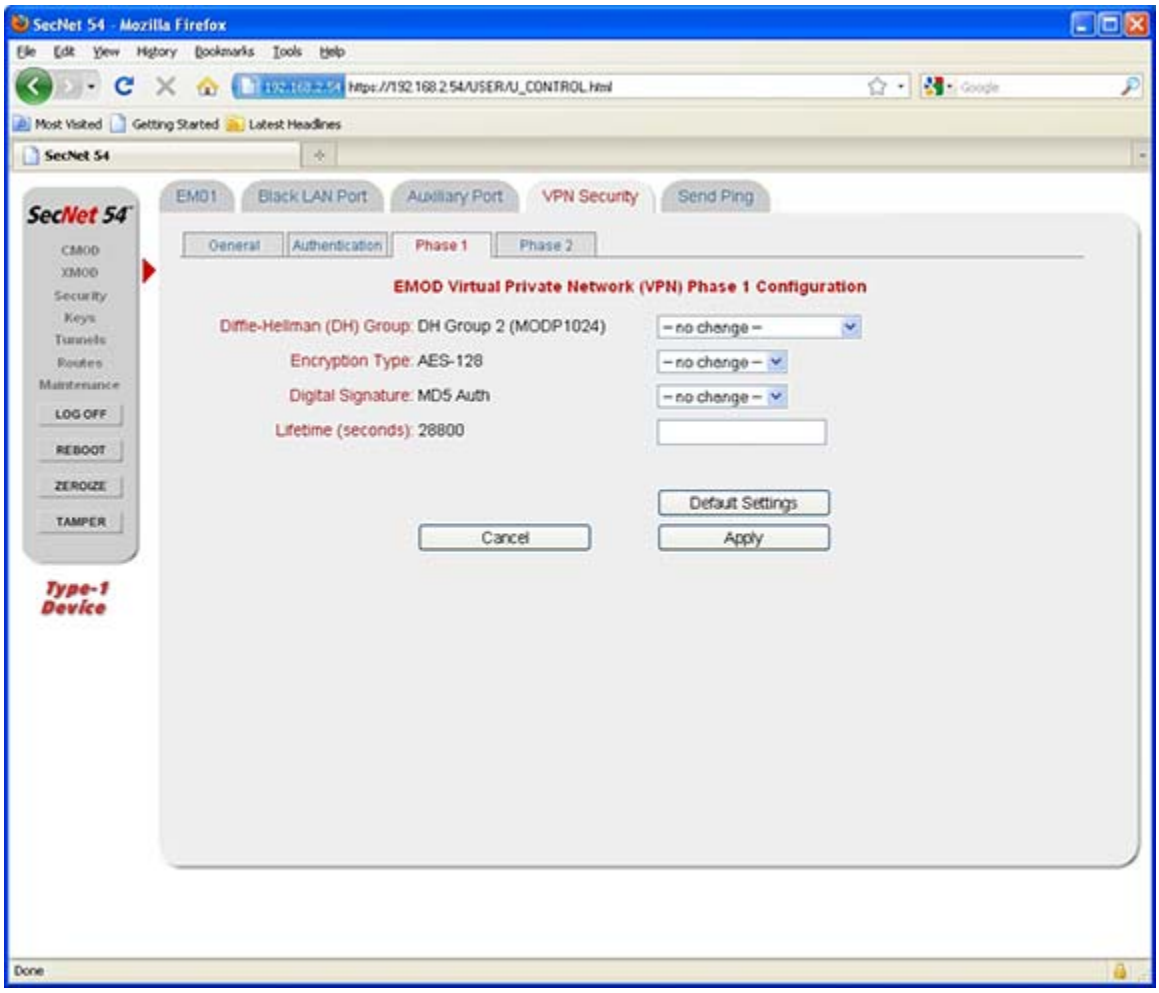
UNCLASSIFIED//FOUO



UNCLASSIFIED//FOUO

(U//FOUO) Selecting the **Configure** button displays the **RMOD Virtual Private Network (VPN) Phase 1 Configuration** page.

UNCLASSIFIED//FOUO



UNCLASSIFIED//FOUO

(U//FOUO) The fields on the **Virtual Private Network (VPN) Phase 1 Configuration** page support VPN tunnels for the RM01 wireless radio. The fields and their selectable values are listed below:

a. (U) Diffie-Hellman (DH) Group

- (U//FOUO) DH Group 2 (MODP1024) - More Modular Exponential (MODP)
- (U//FOUO) DH Group 5 (MODP1536)

b. (U) Encryption Type

- (U//FOUO) 3 DES - 168-bit Triple Data Encryption Standard
- (U//FOUO) AES-128 (-192, -256) - AES -128-bit, 192-bit, and 256-bit

c. (U) Digital Signature

- (U//FOUO) MD5 Auth - Message-Digest Algorithm (MD5 is 128 bites or 16 bytes) Authentication
- (U//FOUO) SHA-1 Auth - Secure Hash Algorithm One (160 bits or 20 bytes) Authentication

d. (U//FOUO) Lifetime (seconds) - This data entry field is how long this end will wait for Phase 1 to complete.

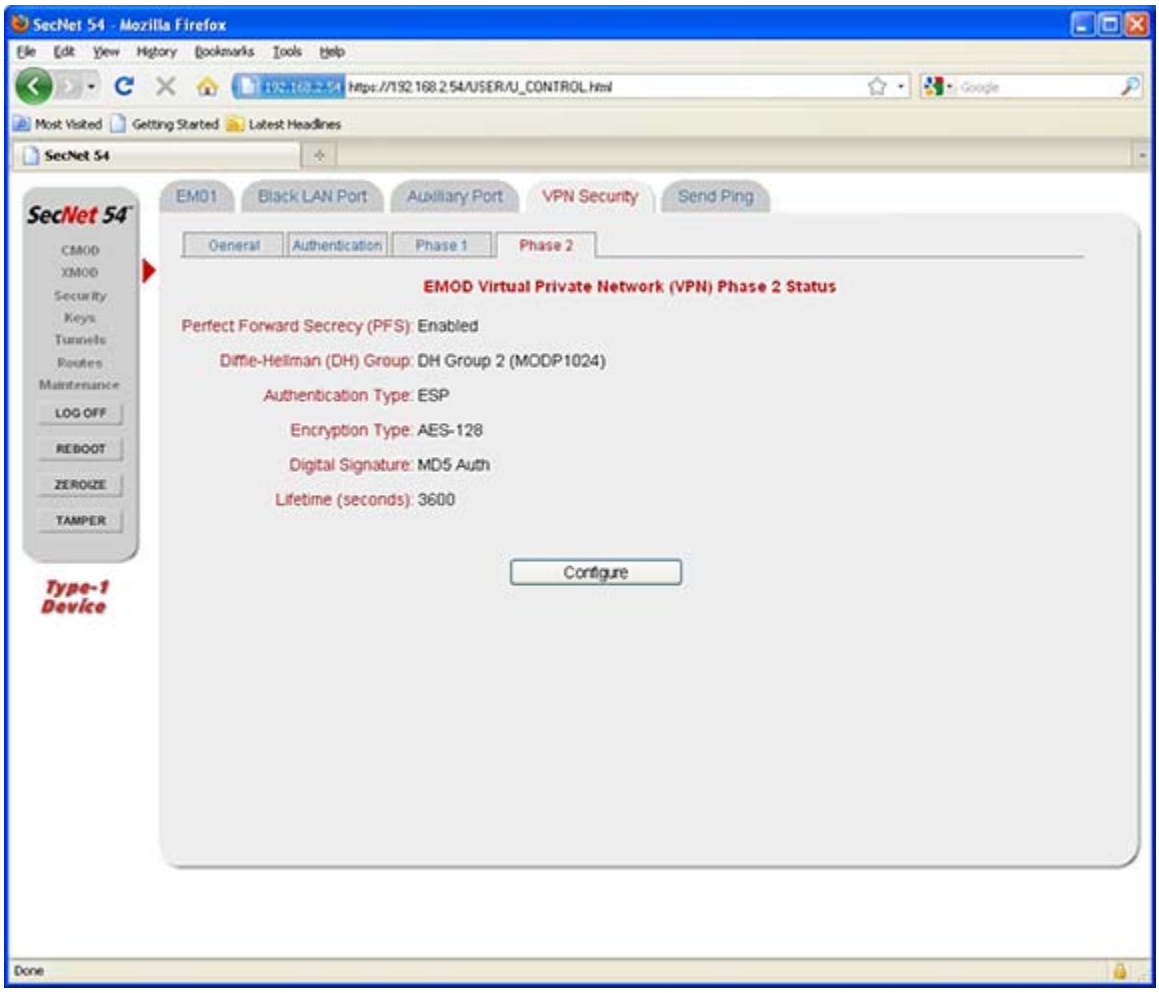
(U//FOUO) Selecting the **Cancel** button removes the entered values and redisplays the **RMOD Virtual Private Network (VPN) Phase 1 Status** page. Selecting the **Default Settings** button populates the fields with the default settings, and selecting the **Apply** button displays the following message and saves any modifications or the default settings, as applicable.

Please wait while your changes are applied...

3-2.6.4.4 (U) Setting RM01 VPN Phase 2 Parameters

(U//FOUO) The **Phase 2** tab displays the **RMOD Virtual Private Network (VPN) Phase 2 Status** page.

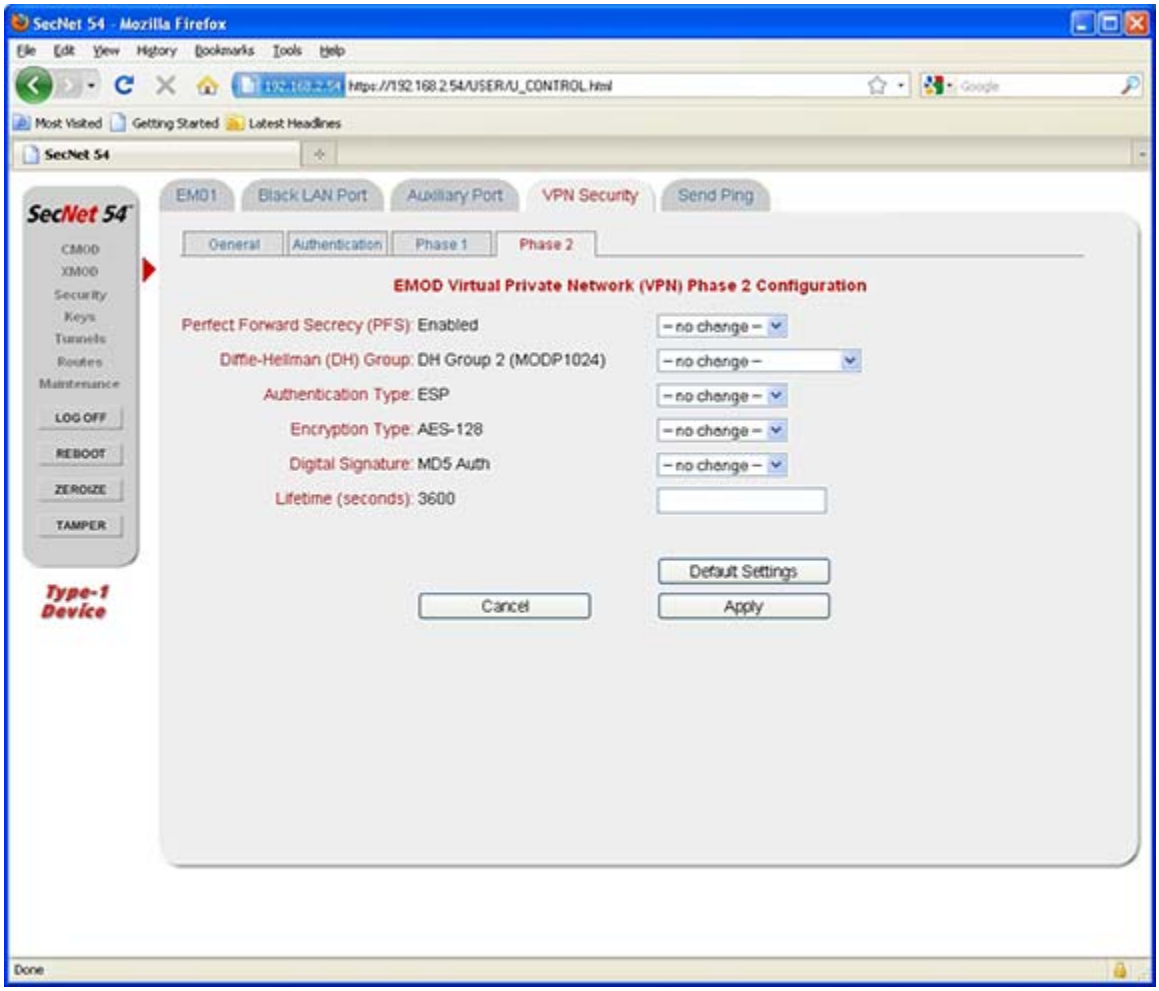
UNCLASSIFIED//FOUO



UNCLASSIFIED//FOUO

(U//FOUO) Selecting the **Configure** button displays the **RMOD Virtual Private Network (VPN) Phase 2 Configuration** page.

UNCLASSIFIED//FOUO



UNCLASSIFIED//FOUO

(U) The fields and their selectable values are listed below:

a. (U//FOUO) Perfect Forward Secrecy (PFS) is Enabled or Disabled. Enabling PFS activates the DH Group data entry field.

b. (U) Diffie-Hellman (DH) Group

- (U//FOUO) DH Group 2 (MODP1024)
- (U//FOUO) DH Group 5 (MODP1536)

c. (U) Authentication Type

- (U//FOUO) ESP - Encapsulation Security Payload (Protocol 50). This selection activates the Encryption Type data entry field.

- (U//FOUO) AH - Authentication Header (Protocol 51). This selection disables the Encryption Type data entry field.

d. (U//FOUO) Encryption Type - Associated with the ESP Authentication Type.

- (U//FOUO) 3 DES - 168-bit Triple Data Encryption Standard
- (U//FOUO) AES-128 (-192, -256) - Advanced Encryption Standard (AES) - 128-bit, 192-bit, and 256-bit

e. (U) Digital Signature

- (U) MD5 Auth - Message-Digest Algorithm Authentication
- (U) SHA-1 Auth - Secure Hash Algorithm Authentication

f. (U) Lifetime (seconds) - This is the length of time the negotiated keys are valid.

(U//FOUO) Selecting the **Cancel** button removes the entered values and redisplays the **RMOD VPN Phase 2 Status** page. Selecting the **Default Settings** button populates the fields with the default settings, and selecting the **Apply** button displays the following message and saves any modifications or the default settings, as applicable:

Please wait while your changes are applied...

3-2.6.4.5 (U) Establishing and Disconnecting RM01 VPN Tunnels

(U//FOUO) Establishing a RM01 VPN tunnel is accomplished by selecting the **Connect VPN** button located on the **RMOD Virtual Private Network (VPN) Status** page.

UNCLASSIFIED//FOUO

UNCLASSIFIED//FOUO

(U//FOUO) The XMOD communications must be enabled prior to connecting the VPN tunnel. When the **Connect VPN** button is selected, the following message displays:

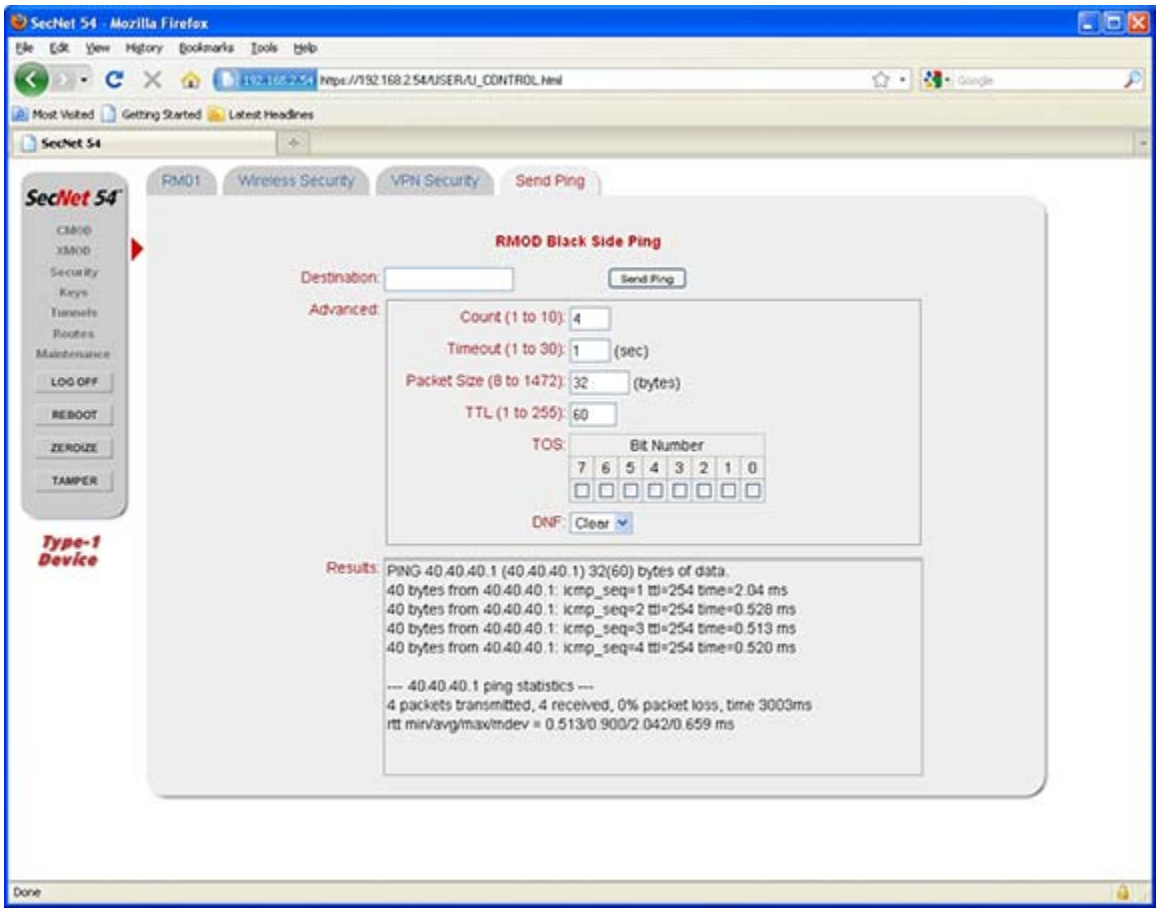
Establishing VPN Tunnel. Please Wait...

(U//FOUO) If no VPN Security network addresses are entered, as described in the previous sections, selecting the **Connect VPN** button displays an error message indicating this. Additionally, if network addresses are entered but there is no preshared key (Section 3-2.6.4.2), an error message also displays. Once the RMOD VPN tunnel is established, the VPN Status area displays a Connected status and the button changes to **Disconnect VPN**. Disconnecting an active VPN tunnel is accomplished by selecting the **Disconnect VPN** button. When the RM01 VPN tunnel is disconnected, the VPN Status area displays a Disconnected status and the button changes to **Connect VPN**.

3.2.6.5 (U) Pinging Another Device on the Black Network

(U//FOUO) Selecting the **Send Ping** tab from the **XMOD** menu displays the **RMOD Black Side Ping** page. From this page the User or Administrator can send a ping from the RM01 to determine if the Black network is set up correctly between a SecNet 54® device another SecNet 54® or HAIPE® device on the Black network.

UNCLASSIFIED//FOUO



UNCLASSIFIED//FOUO

(U//FOUO) When RM01 communication is enabled, the **Send Ping** button is enabled. Sending a ping request requires entering the Destination address of another SecNet 54 device or HAIPE device on the Black network and modifying the values (or leaving the existing values) in the Advanced section. The values entered or selected in the Advanced section indicate the Count (i.e., number of pings to perform), when to Timeout in seconds, Packet Size, Time to Live (TTL), Type of Service (TOS), and Do Not Fragment (DNF). Once the **Send Ping** button is selected, the ping request is sent across the network and displays information in the Results section (in the lower part of the window).

(U//FOUO) The ping Results section (bottom half of the window) displays the ping statistics, which indicates the reply address (destination), number of packets transmitted and received, percentage of loss packets, and the time in milliseconds (ms). If the ping request fails, an error message is displayed, indicating that the Black network is not set up correctly.

UNCLASSIFIED//FOUO

UNCLASSIFIED//FOUO

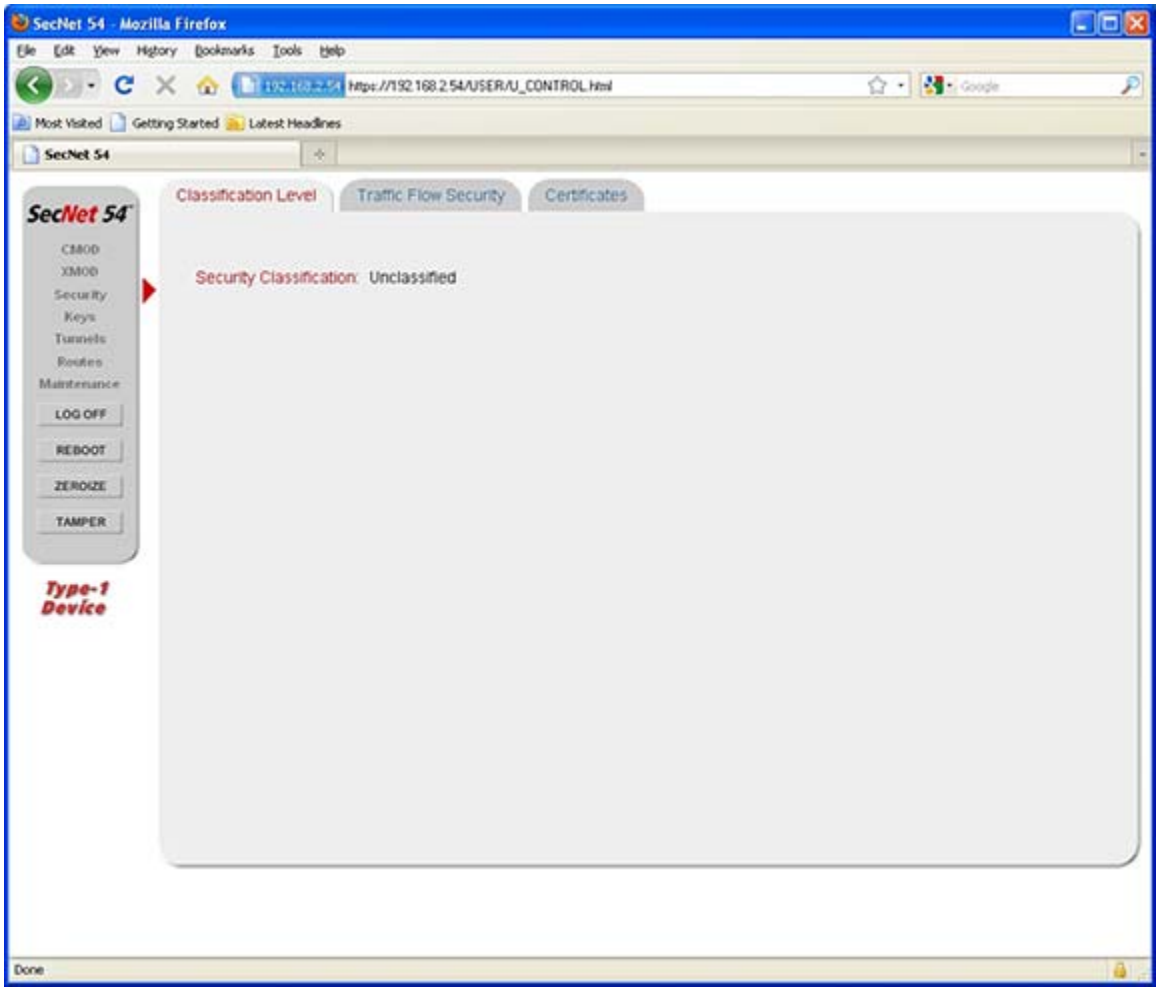
3.2.7 (U) Viewing and Managing Security Settings

(U//FOUO) The **Security** menu option is available with a User and Administrator login. The User has limited privileges and the Administrator has all **Security** menu privileges.

3.2.7.1 (U) Viewing the Device Classification Level

(U//FOUO) The **Classification Level** tab displays the **Security Classification** status page with the current security classification. When loading keys and vectors into the device, the Administrator must ensure that the keys and vectors match the classification level of the device. The Security Classification level is view only to the User.

UNCLASSIFIED//FOUO



UNCLASSIFIED//FOUO

(U//FOUO) The device's security classification is set to one of five levels, Top Secret, Secret, Confidential, Unclassified, and Inhibit. Inhibit is the factory default setting.

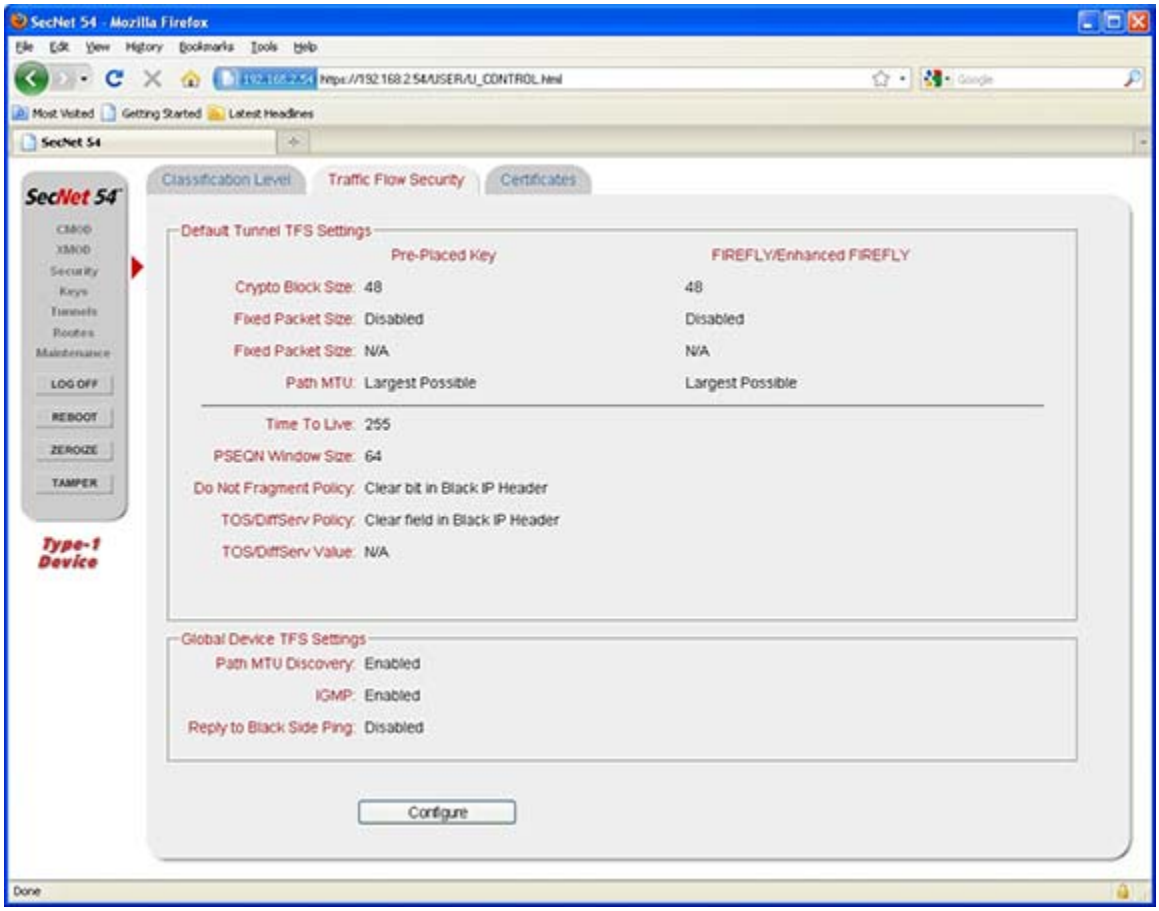
NOTE

(U//FOUO) When the Administrator changes the classification level of a device, all PPKs and vectors that do not match the new classification are deleted and the tunnels are removed that are using the deleted vectors and PPKs.

3.2.7.2 (U) Viewing the Traffic Flow Security (TFS) Settings

(U//FOUO) The Traffic **Flow Security** tab displays the current settings of the Default Tunnel TFS and the Global Device TFS. Only an Administrator can change the TFS network settings.

UNCLASSIFIED//FOUO



UNCLASSIFIED//FOUO

(U) The following is a listing and descriptions of the TFS settings.

1. (U) Default Tunnel TFS Settings (Pre-Placed Key and FIREFLY/Enhanced FIREFLY):

   a. (U//FOUO) Crypto Block Size - One of the following crypto block size values is selected for PPK tunnels and is used as a default on a per tunnel basis: 4-byte, 8-byte, or 48-byte. One or a combination of the crypto block sizes (4-byte, 8-byte, or 48-byte) are selected for IKE tunnels. Dynamic Discovery tunnels use the selected TFS values for IKE tunnels and negotiate the most secure crypto block size based on the values selected.

   b. (U) Fixed Packet

- (U//FOUO) Enabled: When selected, the list box associated with the Fixed Packet Size field is activated, allowing the size of the fixed size packets to be set. The range of values is based on the byte size selected from the Crypto Block Size check box.
- (U//FOUO) Disabled: When the Fixed Packet Size setting is disabled, the list box associated with the Path Maximum Transfer Unit (MTU) field is activated and the Path MTU can be set.

c. (U//FOUO) Fixed Packet Size - The following bytes are selected from the pull down list box: 1424, 1376, 1328, 1280, 1232, 1184, 1136, 1088, 1040, 992, 896, 848, 800, 752, 704, 656, 608, 560, 512, 464, 416, 368, 320, 272, 224, 176, 128, and 80.

d. (U//FOUO) Path MTU - The Path MTU is the size in bytes of the largest packet that can traverse the path between two hosts without fragmentation. The Path MTU range available for the Red side of a SecNet 54® is from 1424 bytes down to 80 bytes, in 48 byte increments. The Black Path MTU is automatically calculated from the Red PMTU by adding 60 bytes to account for the Encapsulated Security Payload (ESP) header that is added to all Red packets when encrypted in the HAIPE format; so the Black Path MTU = Red Path MTU + 60 bytes. The Black Path MTU is calculated from the manually configured Red Path MTU and is not affected by Internet Control Message Protocol (ICMP) messages from the Black network. The values for the Red Path MTU Setting and the Black Path MTU are listed in the following table.

UNCLASSIFIED//FOUO

Red Path MTU Setting	Black Path MTU
80	140
128	188
176	236
224	284
272	332
320	380
368	428
416	476
464	524
512	572
560	620
608	668
656	716
704	764
752	812

Red Path MTU Setting	Black Path MTU
800	860
848	908
896	956
944	1004
992	1052
1040	1100
1088	1148
1136	1196
1184	1244
1232	1292
1280	1340
1328	1388
1376	1436
1424	1484
Largest Possible	Largest Possible

UNCLASSIFIED//FOUO

e. (U//FOUO) Time to Live (TTL) - This field of the Black IP Header will be set to the value specified, which is displayed on the **Traffic Flow Security** status page.

f. Packet Sequence Number (PSEQN) - The associated drop-down list box contains the following packet sizes for configuring the PSEQN window size: 64, 128, 192, and 256. The default value of the PSEQN window size is 64 for the default TFS settings for tunnels.

g. (U) Do Not Fragment

- (U//FOUO) Clear Bit in Black IP Header - All outgoing Black packets will have the Do Not Fragment bit set to FALSE (cleared) in the Black IP Header. Note that this is the default setting, as the “Do Not Fragment Policy” should always be set to "Clear" to allow Black-side fragmentation.
- (U//FOUO) Copy Bit from Red to Black IP Header - All outgoing Black packets will have the Do Not Fragment bit set to the same as incoming Red packets.
- (U//FOUO) Set Bit in Black IP Header - All outgoing Black packets will have the Do Not Fragment bit set to TRUE (i.e., Set) in the Black IP Header.

h. (U) TOS/DiffServ Policy

- (U//FOUO) Clear Field in Black IP Header - All outgoing Black packets will have the Type of Service (TOS) field of the Black IP Header set to 0.

- (U//FOUO) Copy Field from Red to Black IP Header - All outgoing Black packets will have the TOS field of the Black IP Header set to the same as incoming Red packets.
- (U//FOUO) Set Field in Black IP Header to a Specific Value - All outgoing Black packets will have the TOS field of the Black IP Header set to the value specified, as selected in the Bit Number section.

i. (U//FOUO) TOS/DiffServ Value - The Bit Number check boxes become active when the TOS/DiffServ Policy is set to “Set Field in Black IP Header to a Specific Value”. When this policy and the selected bit numbers are saved, the bit number is displayed on the **Traffic Flow Security** status page in binary and hexadecimal number format.

2. (U) Global Device TFS Settings

a. (U) Path MTU Discovery -

- (U//FOUO) Enabled: Request Internet Group Management Protocol (IGMP) notification when fragmentation is needed.
- (U//FOUO) Disabled: This is the default setting

b. (U//FOUO) IGMP - The IGMP is a communications protocol used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts to establish multicast group memberships. The IGMP modes of Disabled and Enabled are described below:

- (U//FOUO) Enabled: Both the Red and Black interfaces act in IGMP Host Mode in accordance with RFC2236.
- (U//FOUO) Disabled: No IGMP is generated by the SecNet 54® device. This is the default setting.

c. (U//FOUO) Black Side Reply to Ping -

- (U//FOUO) Enabled: Allows the RM01 to respond to ping requests.
- (U//FOUO) Disabled: Prevents the RM01 from responding to ping requests.

3.2.7.3 (U) Managing Red and Black Security Certificates

(U//FOUO) The KIV-54 package (Section 1.3.1) contains Harris-developed SecNet 54® Red SSL CA and Client Certificates, which must be loaded into the host computer’s Web browser to log into the SecNet 54® configuration Web pages. These certificates do not require additional installation into the SecNet 54® device through the **Security** menu option via the **Certificates** Web pages. Refer to Section 3.2.1 and Appendix G for Harris-developed certificates installation instructions for three common Web browsers. While Harris-developed certificates are installed into the host computer’s Web browsers, customer-developed Red SSL certificates and Black certificates must be uploaded through the **Certificates** Web pages. Customer-developed certificates are not provided by Harris® Corporation

(U//FOUO) Selecting the **Certificates** tab from the **Security** menu option displays two additional subtabs for Red and Black certificates, **CA Certificate** and **Key Pairs**. The Red certificates are used for SSL purposes and allow direct Web access (Section 3.2.2). The Black certificates allow authentication when using the WPA2 Enterprise mode for RM01 wireless security (Section 3-2.6.2.3) and authentication for RM01 VPN tunnels.

(U//FOUO) A total of three CA and six Public/Private Key Pairs (customer-developed) can be uploaded into a device. These nine certificates do not include the Harris-provided SecNet 54® (Red) SSL Certificates.

NOTE

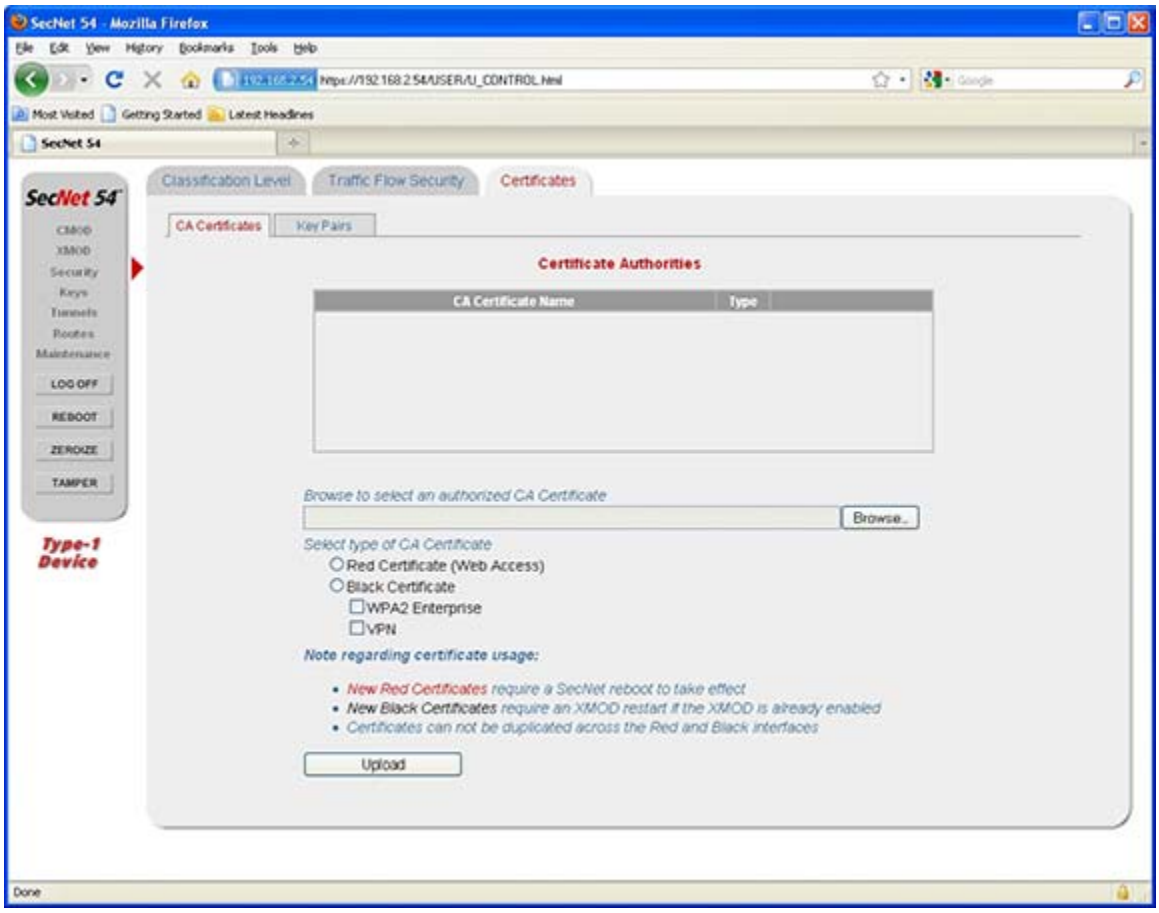
(U//FOUO) A factory reset of the SecNet 54® device will cause the device to revert back to using the Harris® Corporation SecNet 54® SSL CA and Public/Private Key Pair Certificates, if installed. Refer to Section 2-3.1.2.2 for additional information about a factory reset.

(U//FOUO) The following sections describe how to upload the Red and Black CA Certificates and Key Pairs into the SecNet 54® device. The file names and certificates illustrated are examples only.

3-2.7.3.1 (U) Uploading Red CA Certificates into the SecNet 54® Device

(U//FOUO) The **CA Certificates** tab is the default display. From this page the customer-developed Red CA Certificate is loaded. The Red CA certificate must match the Red Client certificate used by the host computer's Web browser.

UNCLASSIFIED//FOUO



UNCLASSIFIED//FOUO

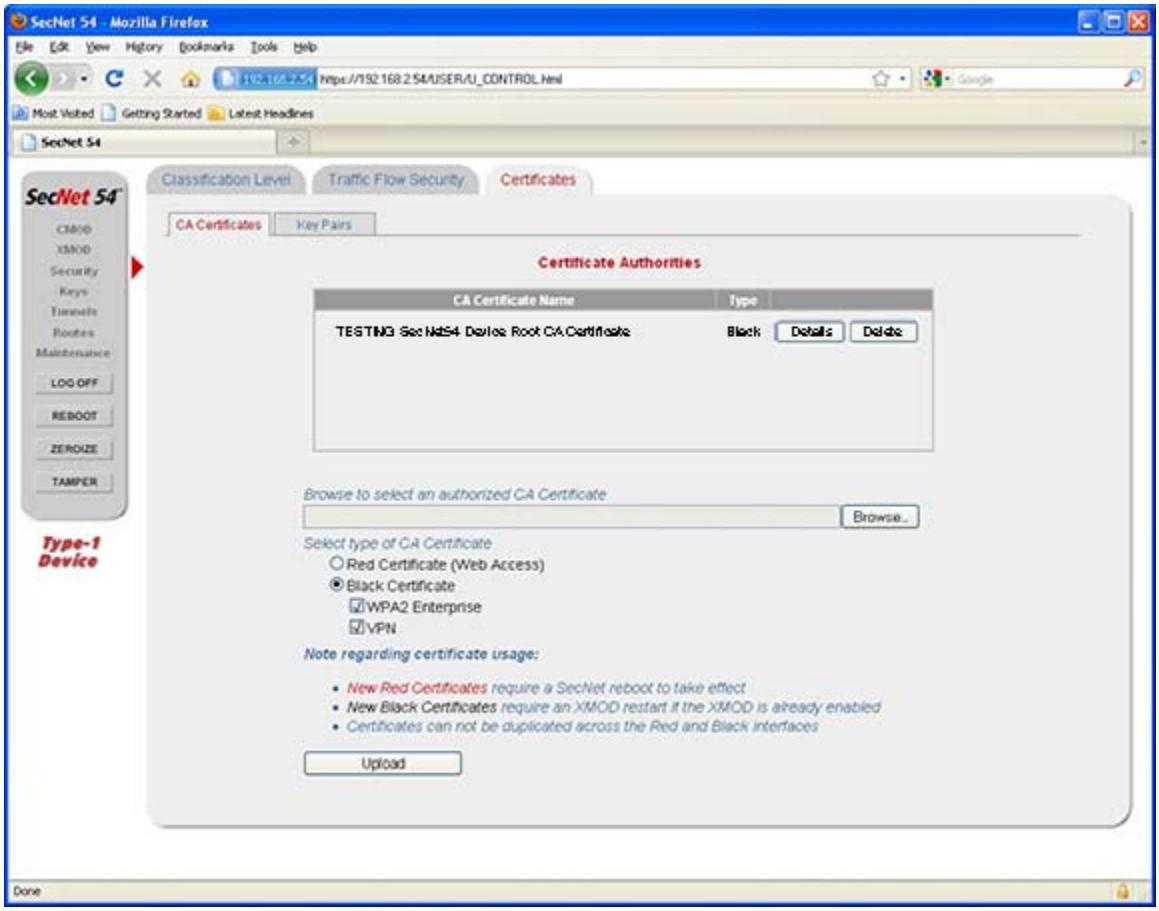
(U//FOUO) Any existing CA certificates are displayed in the Certificate Authorities table with its associated Type indicated. Uploading a CA certificate requires selecting the radio button for “Red Certificate (Web Access)” and selecting the **Browse...** button to display the **Choose file** window from which to locate uninstalled certificate file. In this example the CA Certificate file has a “.pem” file extension.

(U//FOUO) Double-clicking the selected file displays its location in the data entry field of the **Browse...** button on the **Certificate Authorities** tab page. Selecting the **Upload** button on the tab page displays the following message:

Please wait while your changes are being applied....

(U//FOUO) When the “.pem” file is installed into the SecNet 54® device, it is viewable in the Certificates Authorities table listing. The following figure is an example of a Red SSL CA Certificate loaded into the SecNet 54® device.

UNCLASSIFIED//FOUO



UNCLASSIFIED//FOUO

(U//FOUO) Note that when uploading the file, if the **Upload** button is selected prior to selecting a file, the following message displays:

No CA Certificate file was found.

(U//FOUO) Once the file is loaded and displayed in the Certificates Authorities table, a **Details** and **Delete** button appears next to the certificate. selecting the **Details** button associated with the CA Certificate displays the **Certificate Details** window in the Web browser.

UNCLASSIFIED//FOUO

UNCLASSIFIED//FOUO

(U//FOUO) The scrollable window displays information about the certificate, including data such as the version number, serial number, and issuer. Selecting the **OK** button, located at the bottom of the window, closes the window.

(U//FOUO) Selecting the **Delete** button associated with the CA Certificate displays the following message:

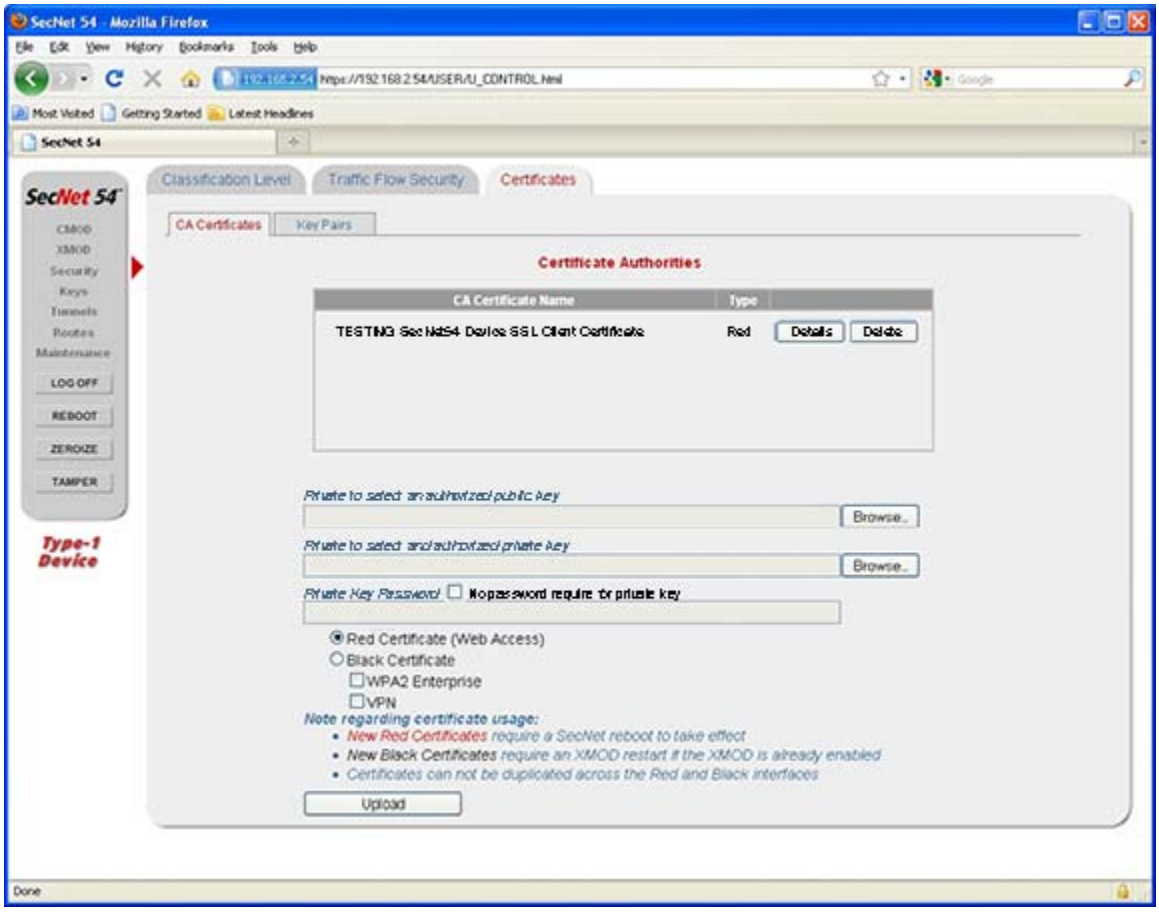
Please wait while your changes are applied...

(U//FOUO) The Certificate Authorities table updates with the CA Certificate removed.

3-2.7.3.2 (U) Uploading Red Public/Private Key Pairs into a SecNet 54® Device

(U//FOUO) Selecting the **Key Pairs** tab displays the **Public/Private Key Pairs** page.

UNCLASSIFIED//FOUO



UNCLASSIFIED//FOUO

(U//FOUO) Uploading the Red key pair requires selecting the radio button for “Red Certificate (Web Access)”. After the check box selection, selecting each **Choose File** button displays the **Choose file** window from which to locate the Public and Private Keys. The Public Key is the Client Certificate and the Private Key is a SSL Client Key. The Private Key is used with or without a password. If a password is not required for the Private Key, the checkbox can be selected, making this field unselectable.

(U//FOUO) Both the Public and Private Key files have “.pem” file extensions, and the following names and password are used:

- (U//FOUO) The Public Key name is **Custom_SSL_Public Key_Client.pem**
- (U//FOUO) The Private Key file name (with password) is **Custom_SSL_Client.pem** (password: **cert_pswd**)

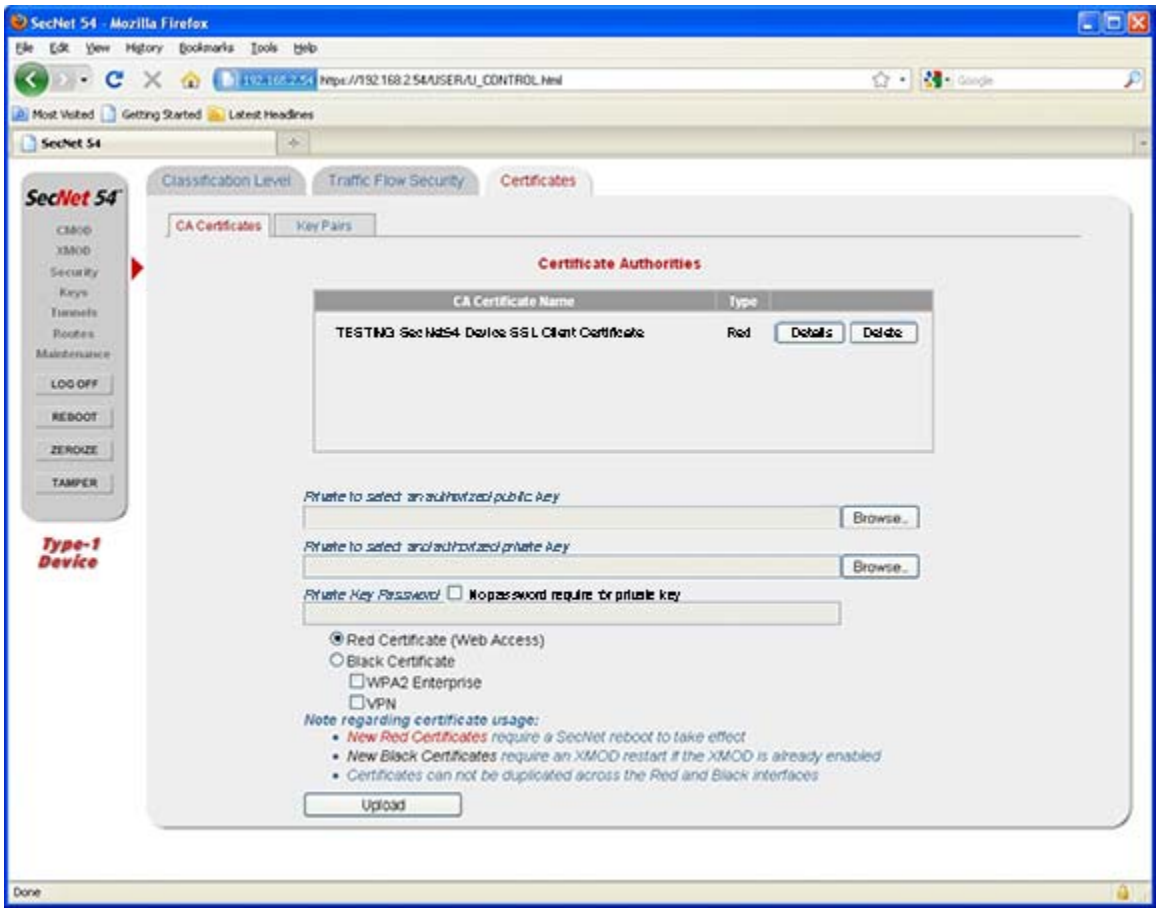
- (U//FOUO) The Private Key file name without a password is **Custom_SSL_Client_nopwd.pem**

(U//FOUO) Double-clicking the selected file displays its location in the data entry field of the **Browse...** button on the **Key Pairs** tab page. Selecting the **Upload** button displays the following message:

Please wait while your changing are being applied...

(U//FOUO) When the file is loaded into the SecNet 54® device, it is viewable in the Public/Private Key Pairs table listing.

UNCLASSIFIED//FOUO



UNCLASSIFIED//FOUO

(U//FOUO) Note that when uploading a certificate file, if the **Upload** button is selected prior to selecting a file, the following message displays:

File entered was not a valid key.

(U//FOUO) Once the file is loaded and displayed in the Public/Private Key Pairs table, a **Details** and a **Delete** button appears next to the certificate. Selecting the **Details** button displays the **Certificate Details** window in the Web browser.

UNCLASSIFIED//FOUO

UNCLASSIFIED//FOUO

(U//FOUO) The scrollable window displays information about the certificate, including data such as the version number, serial number, and issuer. Selecting the **OK** button, located at the bottom of the window, closes the window.

(U//FOUO) The newly loaded certificates are operational after a reboot of the SecNet 54 device. Refer to Section 3.2.13 for the device reboot description.

(U//FOUO) Selecting the **Delete** button associated with the Client Certificate displays the following message:

Please wait while your changes are applied...

(U//FOUO) The Public/Private Key Pairs table updates with the certificate removed.

3-2.7.3.3 (U) Uploading Black CA Certificates and Key Pairs into a SecNet 54® Device

(U//FOUO) The upload process for the Black CA Certificate and Public/Private Key Pairs is almost identical to the Red certificates upload process, as described in Sections 3-2.7.3.1 and 3-2.7.3.2. The difference is that the “Black Certificate” radio button must be selected on the certificate pages versus the “Red Certificate” radio button. Additionally, since one or both Black certificates (WPA2 Enterprise and/or VPN) can be loaded into a device, an extra step involves selecting one or both check boxes underneath the “Black Certificate” radio button, as illustrated.

UNCLASSIFIED//FOUO

UNCLASSIFIED//FOUO

UNCLASSIFIED//FOUO

UNCLASSIFIED//FOUO

(U//FOUO) Refer to Sections 3-2.7.3.1 and 3-2.7.3.2 for descriptions of uploading the files. Note that WPA2 Enterprise and VPN CA and Key Pair Certificates' filenames are customer specific. For the certificates to become operational, a reboot of the XMOD is required (Section 3.2.13) if XMOD communications are enabled (Section 3.2.6.1).

3-2.7.3.4 (U) Logging into the Device with Expired Red SSL Certificates

(U//FOUO) When the Harris-developed or customer-developed SSL Server or Client certificate expires, access to the configuration Web pages is denied. Attempting to log in displays an error indicating a secure connection failure and an expired certificate. Although the certificate has expired, the Web browsers provide a means to access the SecNet 54® Web pages using the expired certificates.

NOTE

Access to the SecNet 54® configuration Web pages is denied when the customer-developed certificates are corrupt or invalid. The SecNet 54® device does not revert to the default Harris® SecNet 54® certificates when this occurs. However, the invalid certificates can be de-installed and Harris SSL certificates loaded via the Web browser (refer to Appendix G). Harris® certificates are located on the SecNet® Applications CD (refer to Section 1.3.1).

The following examples illustrate errors displayed when using the IE and Mozilla Firefox Web browsers to access the configuration Web pages with an expired SSL certificate. When attempting the Log into the Web pages using the IE Web browser, the **Security Alert** window displays.

UNCLASSIFIED

UNCLASSIFIED

(U//FOUO) Selecting the **View Certificate** button displays the certificate for verification, and selecting the **Yes** button allows access to the configuration Web page **DEVICE LOGIN** window. Refer to Section 3.2.2.3 for the window description.

(U) When attempting to log into the Web pages using the Mozilla Firefox Web browser, the **Secure Connection Failed** window displays.

UNCLASSIFIED//FOUO

UNCLASSIFIED//FOUO

(U) Selecting the **Or you can add an exception...** hyperlink updates the window with two option buttons.

UNCLASSIFIED

UNCLASSIFIED

(U//FOUO) Selecting the **Get me out of here!** button removes the window, and selecting the **Add Exception...** button displays the **Add Security Exception** window.

UNCLASSIFIED

UNCLASSIFIED

(U//FOUO) The expired certificate is viewable by using the **Get Certificate** button to locate the Server (i.e., the SecNet 54® device). Selecting the **View...** button displays the expired certificate for verification. Finally, by selecting the "Permanently store this exception" check box and the **Confirm Security Exception** button, the Server certificate is accepted to access the **DEVICE LOGIN** window. Refer to Section 3.2.2.3 for the window description.

3.2.8 (U) Viewing the Loaded PPKs, FIREFLY Vectors, and P3 dePAC Moduli

(U//FOUO) Key management is an Administrator login privilege. Users can view loaded PPKs, FIREFLY Vectors, PPK Chains, and P3 Base and Alternate dePAC Moduli, but Users have no key management privileges. The **Keys** menu option provides access to view the PPKs, vectors, chains, and moduli. The SecNet 54® device can support up to 512 PPKs, 16 FIREFLY Vectors, one Base P3 dePAC Moduli, and six Alternate P3 dePAC Moduli.

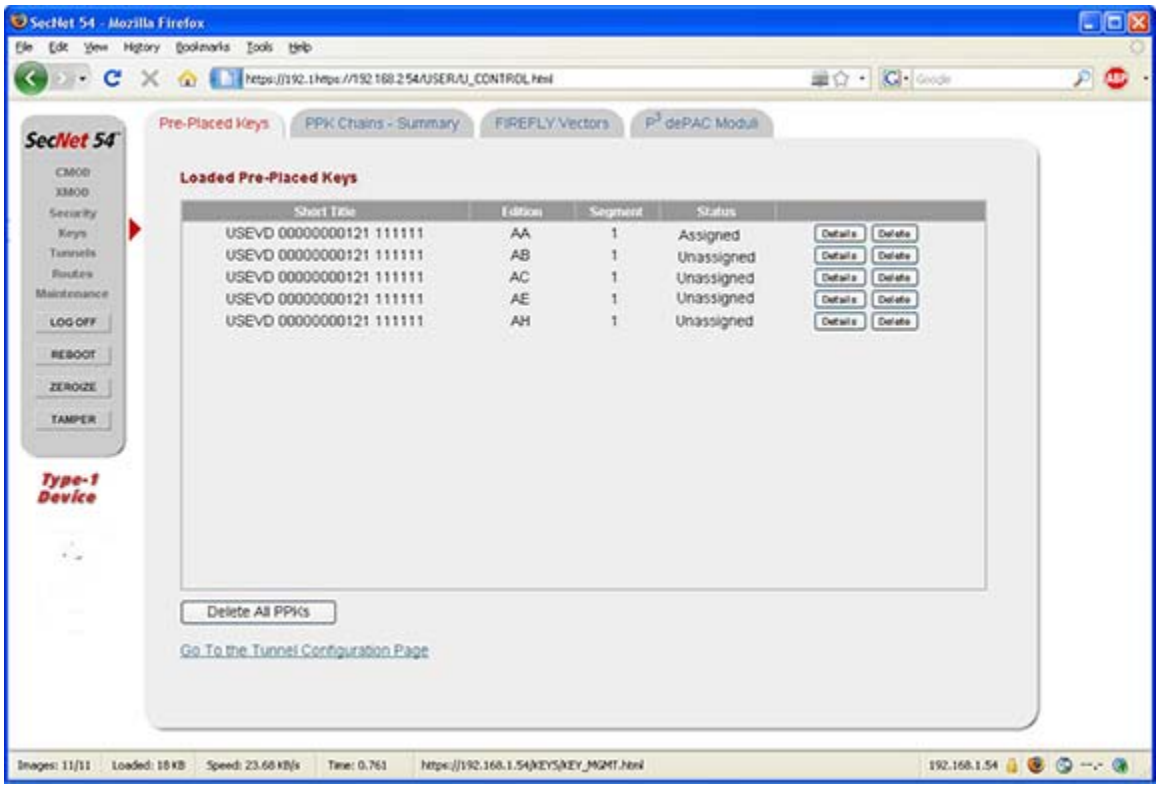
(U//FOUO) The use of P3 Base and Alternate dePAC Moduli supports the HAIPE® Foreign Interoperability Program. FIREFLY Vectors are Positive Access Controlled (PACed) with a specific P3 dePAC Moduli. When the FIRE Vector is loaded into a device, a stored moduli is required to process the vector. The KIV-54 attempts to dePAC the FIREFLY Vector with the Base P3 dePAC Moduli and possibly any Alternate P3 Moduli that may be stored.

(U//FOUO) Once PPKs are loaded, they may be assigned to PPK Chains. Each PPK Chain may then be used to provide keys for one or more tunnels (Administrator login privilege). All PPKs are required to be assigned to a PPK Chain. The PPKs, PPK Chains, and FIREFLY Vectors are retained during power cycles unless they are expired. P3 dePAC Moduli are also retained during power cycles.

3.2.8.1 (U) Viewing the Pre-Placed Keys and Key Chains

(U//FOUO) Selecting the **Pre-Placed Keys** tab displays the **Loaded Pre-Placed Keys** status page with a listing of the loaded PPKs, their editions, segments, and chain assignment status. Included at the bottom of this page is a Go to the Tunnel Configuration Page hyperlink to view configured tunnels.

UNCLASSIFIED//FOUO



UNCLASSIFIED//FOUO

(U//FOUO) Selecting the PPKs associated **Details** button displays the **Details for Active Key** window.

UNCLASSIFIED//FOUO

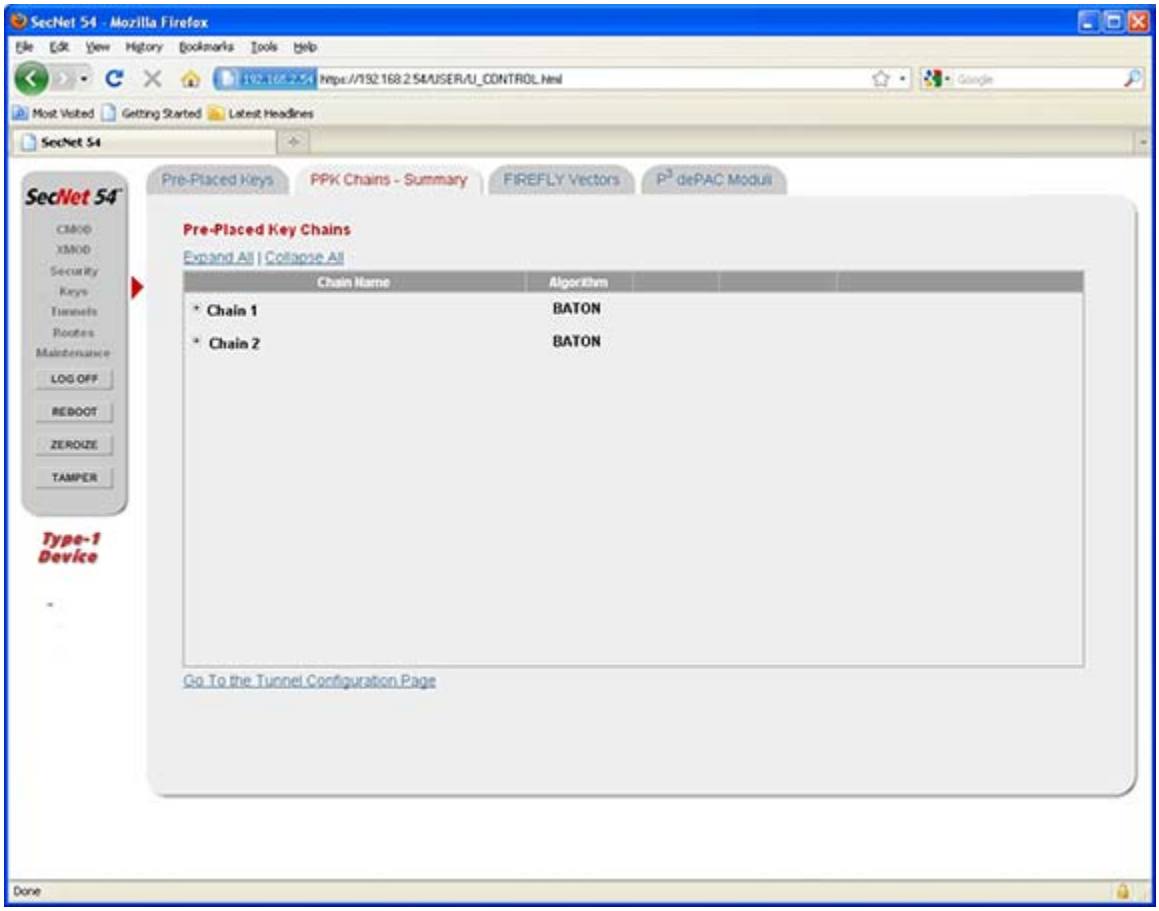
UNCLASSIFIED//FOUO

(U//FOUO) Selecting the **OK** button closes this window. The the Assigned hyperlink on the **Loaded Pre-Placed Keys** page displays the following pop-up window prior to displaying the **PPK Chains-Summary** tab page. The **OK** button removes the pop-up.

UNCLASSIFED//FOUO

UNCLASSIFIED//FOUO

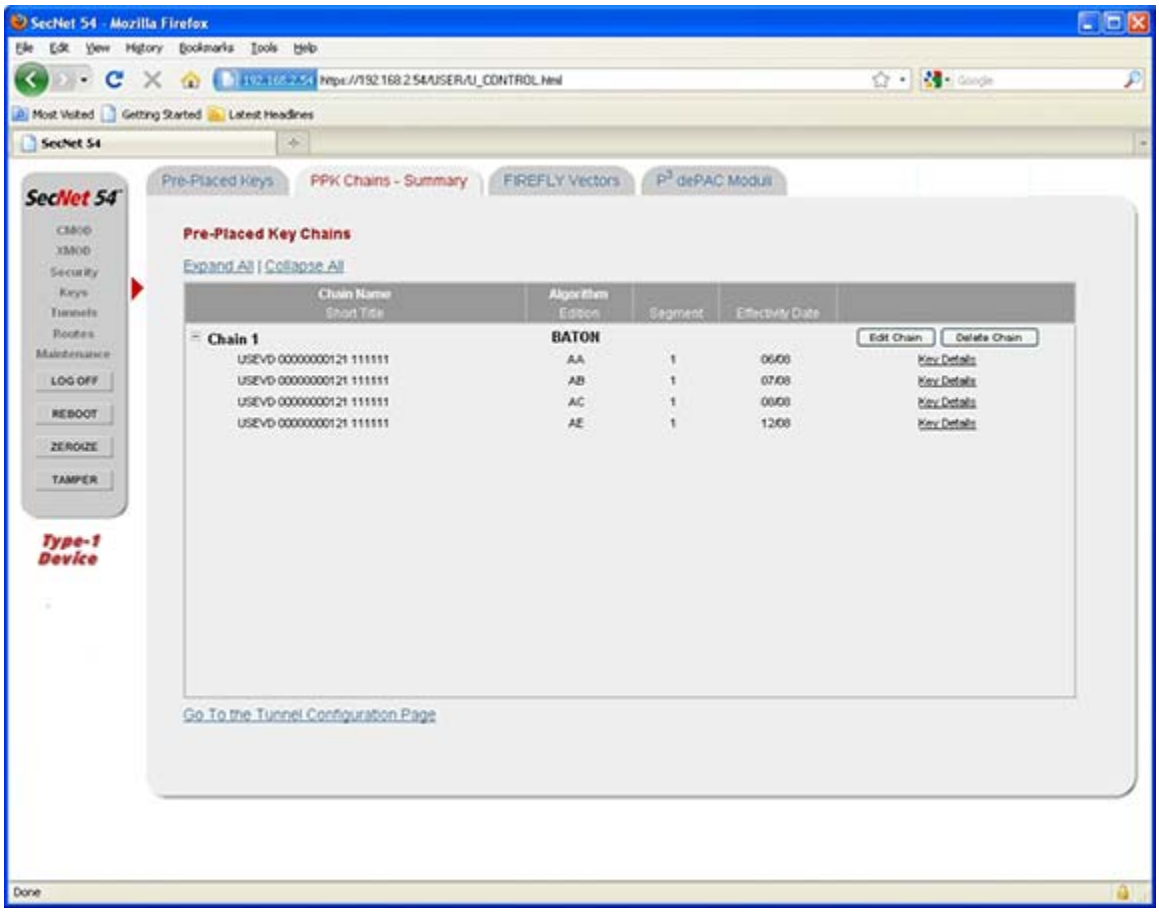
UNCLASSIFIED//FOUO



UNCLASSIFIED//FOUO

(U//FOUO) The **Pre-Placed Key Chains** page displays each PPK Chain Name and their Algorithm method. Selecting the Expand All hyperlink or the plus (+) symbol beside the chain name displays additional column headings associated with the PPK (i.e., Short Title, Edition, Segment, and Effectivity Date). When the chain's keys are displayed, a hyperlink is also available to view additional key details for each key. Selecting Key Details hyperlink displays the **Details for Active Key** window described earlier in this section.

UNCLASSIFIED//FOUO



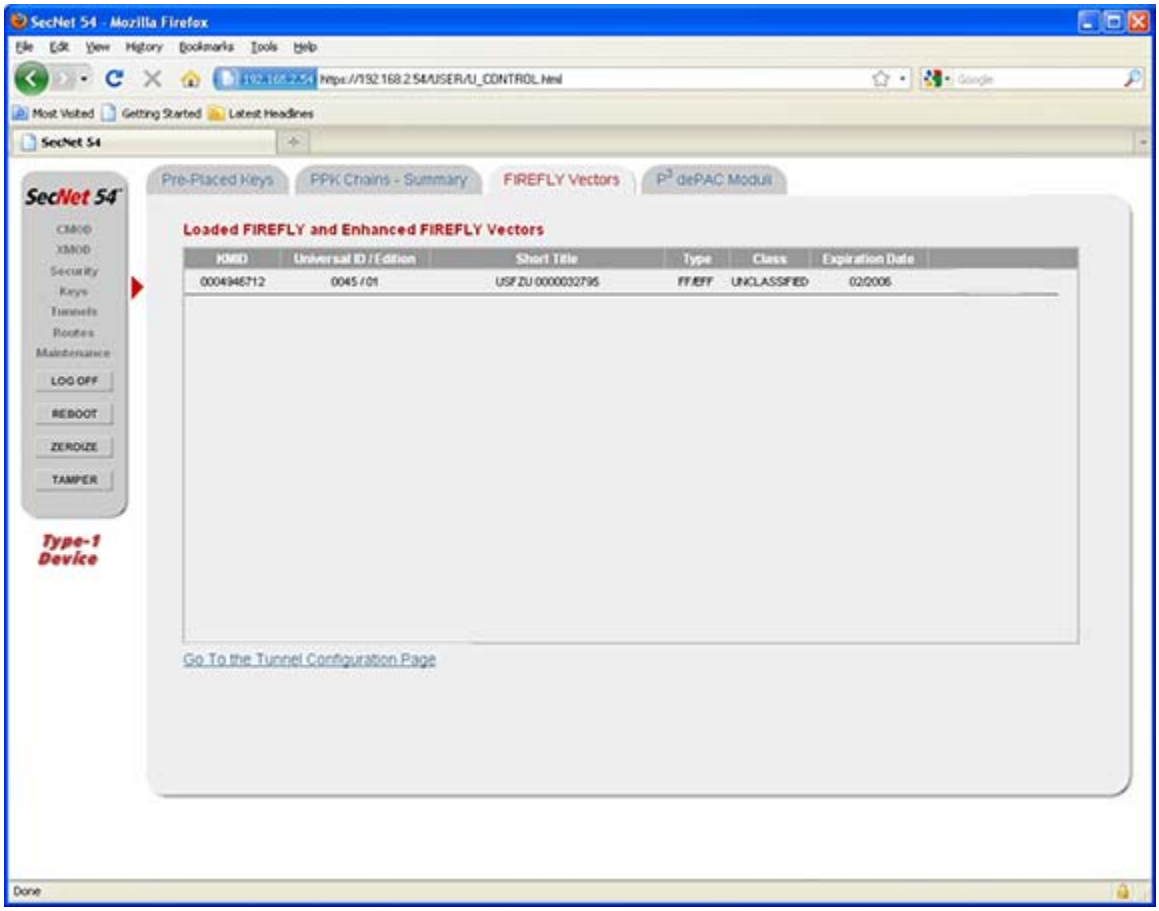
UNCLASSIFIED//FOUO

3.2.8.2 (U) Viewing FIREFLY Vectors

(U//FOUO) Unlike PPKs, in which both HAIPE® devices share a pre-established, pre-configured traffic key, the HAIPE® Internet Key Exchange (IKE) FIREFLY process uses a protocol that exchanges six or more messages to establish a key.

(U//FOUO) FIREFLY is a technique that uses a protocol exchange to electronically negotiate Traffic Encryption Keys (TEKs) using pre-placed key generation material, called vectors, between two independent nodes without further intervention. Once the Administrator loads the FIREFLY Vector, it attempts to dePAC with a stored P^3 Base dePAC Moduli (or Alternate). A stored moduli is required to process the FIREFLY Vector for the creation of a Community of Interest (COI). Afterwards, a one time configuration of the device is performed to set up Dynamic Discovery and HAIPE® IKE parameters enabling the SecNet 54® to communicate with any HAIPE® device within a COI. The COIs are also configured by the Administrator. Dynamic Discovery COIs are described in Section 3.2.9.3

UNCLASSIFIED//FOUO



UNCLASSIFIED//FOUO

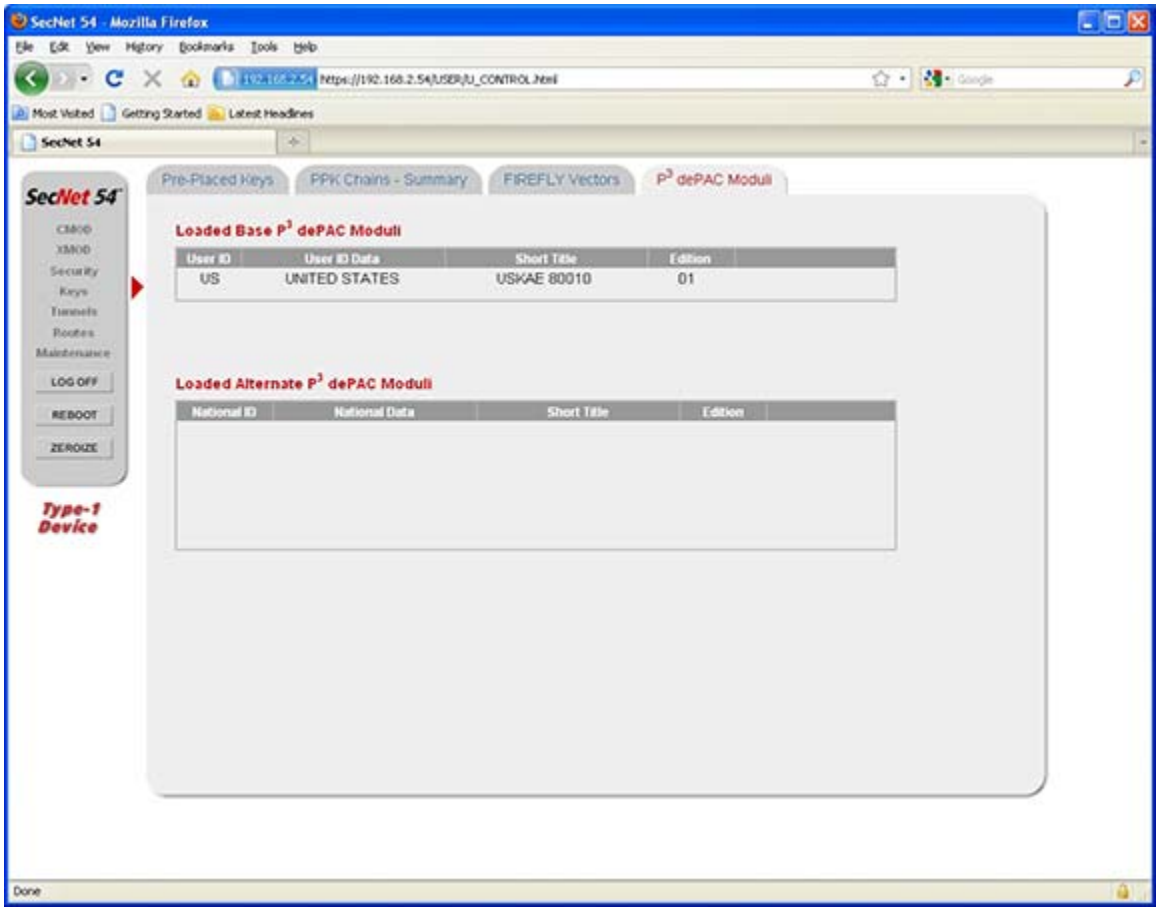
(U//FOUO) Each displayed FIREFLY Vector is identified by a Key Management Identification (KMID) number, which is a 10 digit decimal number of the unique key ID assigned by the Electronic Key Management System (EKMS) Central Facility (CF). This ID only displays for a HAIPE® IKE tunnel, using a FIREFLY key, when the tunnel is established with the destination HAIPE® device.

(U//FOUO) The Universal ID consists of four standard ASCII characters from 0000 to 9999, and the Universal Edition consists of two standard ASCII characters from 00 to 99. Displayed also is the security classification level (Class) and Expiration Date of the FIREFLY Vector. An Alert is displayed on the **Current Status** page (Section 3.2.5.1) 55 minutes prior to a FIREFLY key expiring.

3.2.8.3 (U) Viewing P^3 dePAC Moduli

(U//FOUO) The **P^3 dePAC Moduli** tab page displays loaded Base and Alternate P^3 dePAC Moduli. P^3 dePAC Moduli allow the creation of Dynamic Discovery COIs. When the Administrator modifies a moduli, the modification causes a change in the COI. Multiple moduli are stored on a device to allow for participation in different COIs.

UNCLASSIFIED//FOUO



UNCLASSIFIED//FOUO

(U//FOUO) The Base P3 Moduli are identified by a User ID, User ID Data, Short Title, and Edition, and the Alternate P3 dePAC Moduli are identified by a National ID, National Data, Short Title, and Edition.

NOTE

When the Administrator deletes the Base P3 dePAC Moduli, all loaded P3 dePAC Moduli, FIREFLY Vectors, associated MTEKs, and all TEKs are deleted, and the SecNet 54® device must be returned to the factory to reload the Base P3 dePAC Moduli. Although the Base P3 dePAC Moduli are deleted, the Administrator can load additional Alternate P3 dePAC Moduli.

3.2.9 (U) Viewing Tunnel Configurations for Cryptographic Devices

(U//FOUO) A HAIPE® tunnel is created by the Administrator from the configuration Web pages, and they are view only to the User. A HAIPE® tunnel is the pathway carrying Type-1 encrypted information over a Black network from one HAIPE® compliant device (e.g. a SecNet 54® device) to another HAIPE® compliant device. All HAIPE® tunnel types require that the destination device has the same security level as the source (originating) device to establish a tunnel. The SecNet 54® device can support up to 512 bi-directional tunnels.

(U//FOUO) There are limitations on which tunnel type ((i.e., Tunnel traffic type) Unicast, Multicast, and Broadcast) and their directions when applied to specific kinds of tunnels (static PPK, static HAIPE® IKE, and Dynamic Discovery HAIPE® IKE). These are described in the following list.

a. (U//FOUO) Static PPK tunnel - This tunnel uses National Security Agency (NSA) Type-1 Pre-Placed Keys (PPKs), where the HAIPE® device at each end of a tunnel has the same HAIPE® PPK(s) loaded and associated with the static tunnel. This type of tunnel must be manually configured prior to use and is assumed to be established once properly configured. Configuration consists of assigning PPKs to chains, assigning the chains to a set of IP addresses that represent HAIPE® devices on each end of the tunnel, and then assigning the tunnel to a security policy. Static PPK tunnels can be used for Unicast, Broadcast, and Multicast traffic in one or both directions (Receive (RX) only, Transmit (TX) only, or RX/TX). Special Multicast PPK tunnels are used for the Dynamic Discovery process.

b. (U//FOUO) Static HAIPE® IKE tunnel - This tunnel uses NSA Type-1 FIREFLY Vectors, where the HAIPE® device at each end of a tunnel has the same vectors loaded and associated with the static tunnel. This type of tunnel must be configured and manually established prior to use. Static HAIPE® IKE tunnels establish a Main Traffic Encryption Key (MTEK) through a negotiation process with another HAIPE®. The MTEK negotiation is initiated from the Human Machine Interface (HMI) after configuration. Configuration consists of creating a static IKE tunnel using the IP addresses that represent HAIPE® devices on each end of the tunnel, and then assigning the tunnel to a security policy. These tunnels can be used for Unicast Bi-directional traffic. They cannot be used for Multicast or Broadcast traffic.

c. (U//FOUO) Dynamic Discovery HAIPE® IKE tunnel - Like the static HAIPE® IKE tunnel, the Dynamic Discovery HAIPE® IKE tunnel uses NSA Type-1 FIREFLY Vectors, where the HAIPE® device at each end of a tunnel has the same vectors loaded, however, no specific tunnel has to be configured or established prior to use. Like the other types of tunnels, these must also be associated with a security policy, but the HAIPE® Dynamic Discovery process takes care of determining the proper tunnel end point IP addresses, and HAIPE® IKE negotiates the key to use. The Dynamic Discovery and HAIPE® IKE processes are initiated when a packet is received from the Red network that matches a security policy associated with a Dynamic Discovery HAIPE® IKE tunnel. These tunnels can be used for Unicast Bi-directional traffic. They cannot be used for Multicast or Broadcast traffic.

(U//FOUO) Prior to creating tunnels, HAIPE® PPKs and FIREFLY Vectors, as appropriate, must be loaded into the SecNet 54® device.

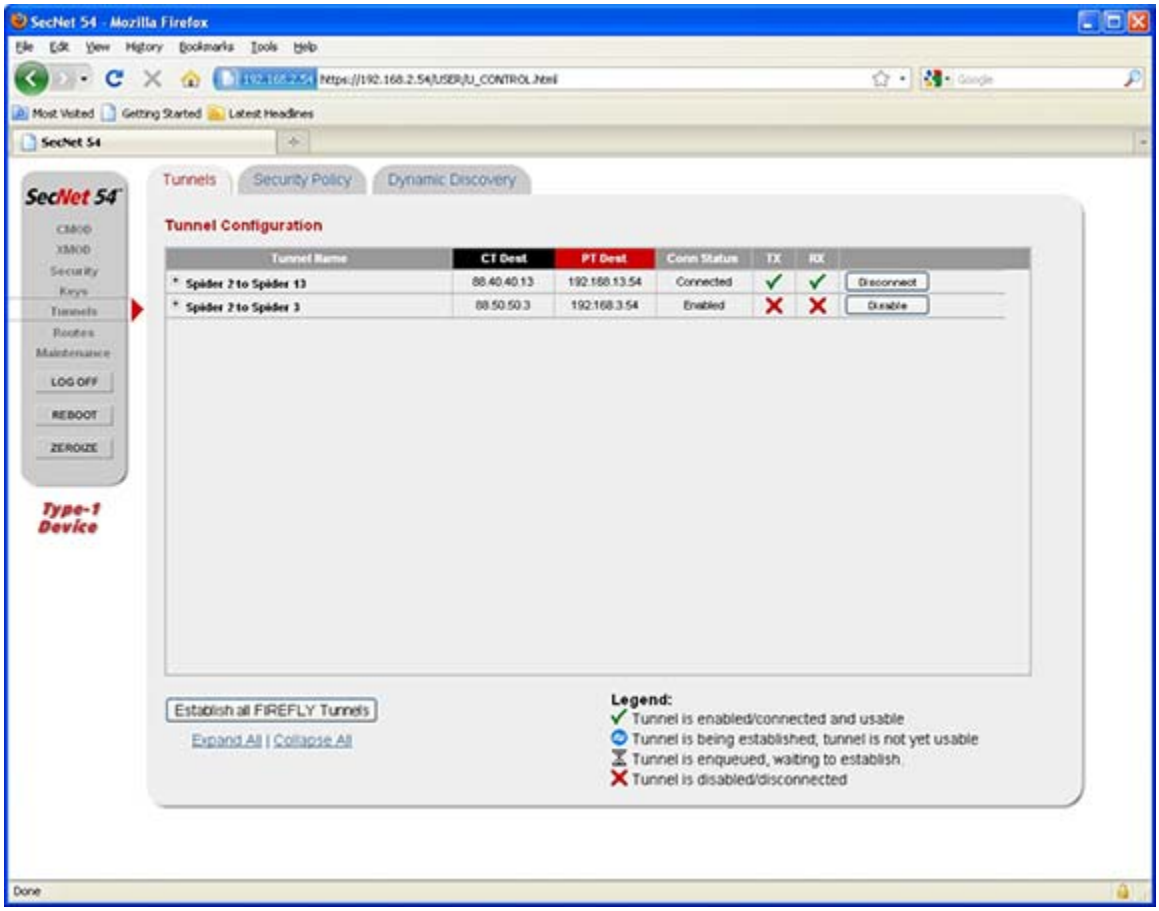
(U//FOUO) After HAIPE® tunnels are created, data can then be sent between classified nodes (i.e., computers or other networked devices) over the HAIPE® devices. When Red data is received by the

SecNet 54® device over its Ethernet interface, from a source node, the data is encrypted and a HAIPE® IPSec header is added. The HAIPE® IPSec encryption secures the data as it travels over the Black network (i.e., the tunnel). When the data is received by the destination SecNet 54® or other HAIPE® device on the other end of the tunnel, the data is decrypted and sent to the Red destination (target) node.

NOTE

(U//FOUO) Tunnels are not required to enable the RM01.

UNCLASSIFIED//FOUO



UNCLASSIFIED//FOUO

(U) The tunnel table contains the following information:

a. (U//FOUO) Tunnel Name - The name assigned by the Administrator when defining the HAIPE® tunnel.

b. (U//FOUO) CT Dest - The Cipher Text Destination is in the outer header of every Packet that travels over the Black network (tunnel) to the HAIPE® Red target node. This is the HAIPE® Black IP address of the end-point SecNet 54® device (i.e., tunnel end-points).

c. (U//FOUO) PT Dest - The Plain Text Destination is the Red IP addresses of the receiving SecNet 54® devices (i.e., tunnel end-point).

d. (U//FOUO) Conn Status - The tunnel's Connectivity Status. The status indicates if the tunnel's connectivity is enabled or connected and ready for use, in progress, disconnected, or disabled. It is associated with the tunnel's ability to transmit (TX) or receive (RX) traffic.

e. (U//FOUO) TX/RX - The TX and RX columns indicate the connection status and display the following symbols as visual indications:

(U//FOUO) When displayed in one or both columns, this symbol indicates that information may be transmitted or received to/from the receiving host. The tunnel is established and enabled.

(U//FOUO) When displayed, as a blue symbol, this indicates that an HAIPE® IKE tunnel is being established and is not yet usable.

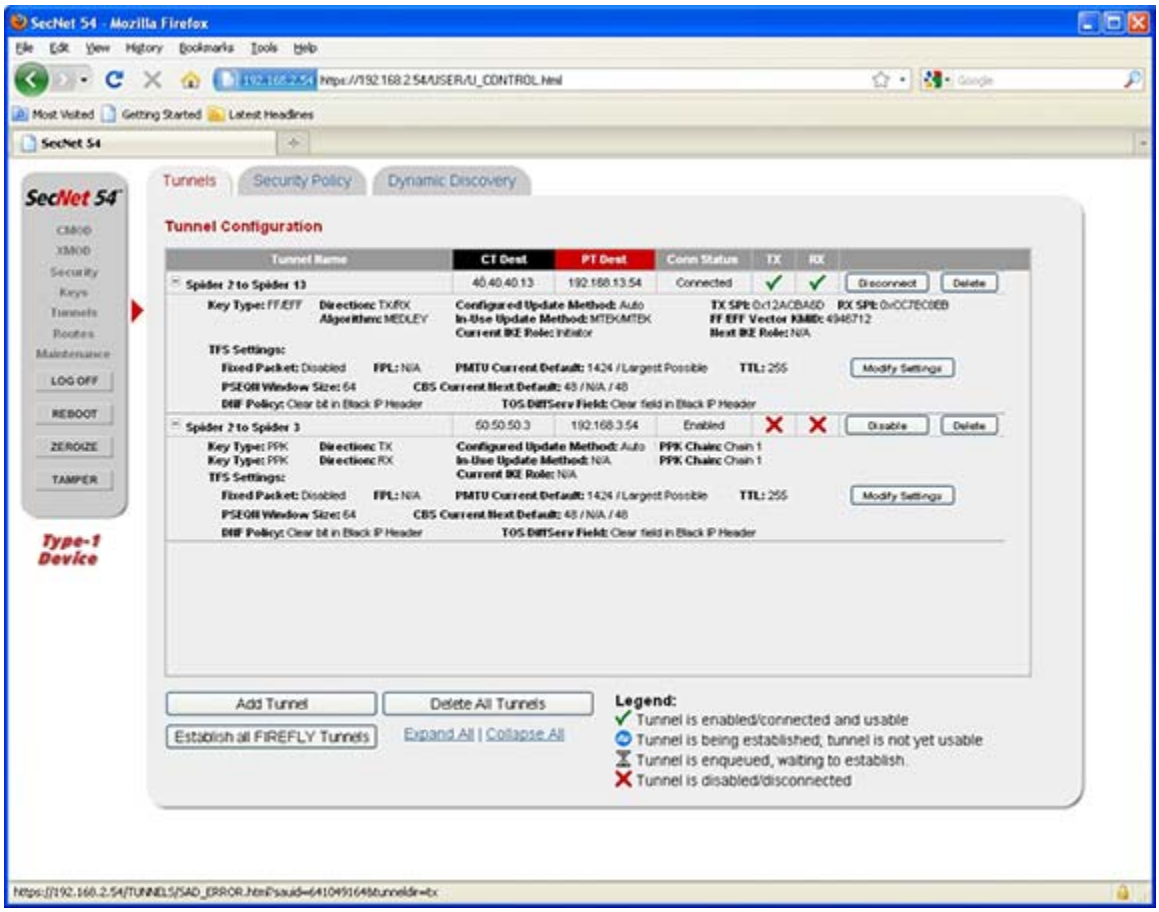
(U//FOUO) When displayed, as a gray symbol, this indicates that the HAIPE® IKE tunnel has not yet begun to establish itself. The tunnel cannot yet receive or transmit information.

(U//FOUO) When displayed in either column, as a red symbol, this indicates that the tunnel is not available to receive or transmit information. The tunnel is disconnected.

(U//FOUO) Tunnels transmit or receive information based on the connectivity type and tunnel direction set when the tunnel is created by the Administrator. Tunnel (traffic) types supported by SecNet 54® devices are Unicast, Multicast, Broadcast (global or subnet), and Discovery. FIREFLY key types only support tunnels with Unicast connectivity.

(U//FOUO) Expanding the tunnel name (i.e., selecting the plus (+) symbol) displays additional data associated with the tunnel. Fields associated with static PPK, static HAIPE® IKE, and Dynamic Discovery HAIPE® IKE tunnels are displayed and described in the following figure and listings.

UNCLASSIFIED//FOUO



UNCLASSIFIED//FOUO

1. (U) Static PPK Tunnel Data Descriptions

   a. (U//FOUO) Key Type - The Key Type is PPK.

   b. (U//FOUO) Direction - The PPK tunnel routes traffic in one or both directions (TX only, RX only, or TX/RX) as determined by the tunnel traffic type (Unicast, Multicast, or Broadcast).

   c. (U//FOUO) Security Parameter Index (SPI) - The SPI is a 32-bit value used to identify the Security Association (SA) at the receiving HAIPE® device. The SPI is developed during the PPK association setup. Prior to a PPK expiring, a changeover notification is displayed on the **Current Status** page as an alert (Section 3.2.5.1). The alert is logged in the audit log, and a second SPI value displays (a 55 minute time-frame) for both TX and RX, if both are applicable. The word “Next” also displays beside the connectivity direction of the newly acquired SPI. During changeover, data may be received on either the Current or the Next SPIs. However, data that is transmitted is always done on the Next SPI. Upon exiting the

changeover window, the Current SPIs expire, and the Next SPIs become current and are used to receive and transmit all data.

d. (U//FOUO) Associated PPK Chain - The PPK Chain selected when configuring the tunnel.

e. (U//FOUO) TFS Settings - The default TFS settings for all tunnels or TFS settings that are specific to this tunnel. Refer to Section 3.2.7.2 for descriptions of the TFS settings.

2. (U) Static HAIPE® IKE and Dynamic Discovery HAIPE® IKE Tunnels Data Descriptions:

a. (U//FOUO) Key Type - The Key Type is FIREFLY or Enhanced FIREFLY.

b. (U//FOUO) Direction - The HAIPE® IKE tunnel routes traffic bi-directional (TX/RX) as determined by the tunnel traffic type. HAIPE® IKE tunnels are Unicast.

c. (U//FOUO) Algorithm - The type of algorithm associated with the PPK Chain. Only BATON algorithm can be used with Dynamic Discovery multicast IP addresses.

d. (U//FOUO) Configured Update Method - One of the following update methods selected when configuring the tunnel to negotiate the MTEK: Auto, MTEK/MTEK, or MTEK/Update (ACCORDION).

e. (U//FOUO) In-Use Update Method - The update method currently being used during the MTEK negotiation process. N/A is displayed if the tunnel is disconnected

f. (U//FOUO) TX SPI/RX SPI -The SPI is developed during the HAIPE® IKE exchange. It is only associated with a HAIPE® IKE tunnel if the tunnel is established with the destination HAIPE® device. Prior to a FIREFLY MTEK expiring, a changeover notification is displayed on the **Current Status** page as an alert (Section 3.2.5.1). The alert is logged in the audit log, and a second SPI value displays (a 55 minute time-frame) for both TX and RX, if both are applicable. The word “Next” also displays beside the connectivity direction of the newly acquired SPI. During changeover, data may be received on either the Current or the Next SPIs. However, data that is transmitted is always done on the Next SPI. Upon exiting the changeover window, the Current SPIs expire, and the Next SPIs become current and are used to receive and transmit all data.

g. (U//FOUO) FIREFLY Vector KMID - The FIREFLY Vector is identified by a KMID number. The KMID is displayed when the HAIPE® IKE tunnel is established with the destination HAIPE® device.

h. (U//FOUO) Current IKE Role - This is the role for the currently negotiated FIREFLY tunnel. If the tunnel is not yet established (i.e., disconnected), N/A displays in this field. If the tunnel is established, either Initiator or Responder displays in this field, depending on whether the device initiated the HAIPE® IKE session or responded to a HAIPE® IKE session.

i. (U//FOUO) Next IKE Role - If a new HAIPE® IKE session is being negotiated, the Next IKE Role field displays either Initiator or Responder. N/A displays if no Next MTEK exists. Note that while in the changeover window, two MTEKs exist (Current and Next). The display will show the proper HAIPE® IKE roles for the respective negotiations. When changeover

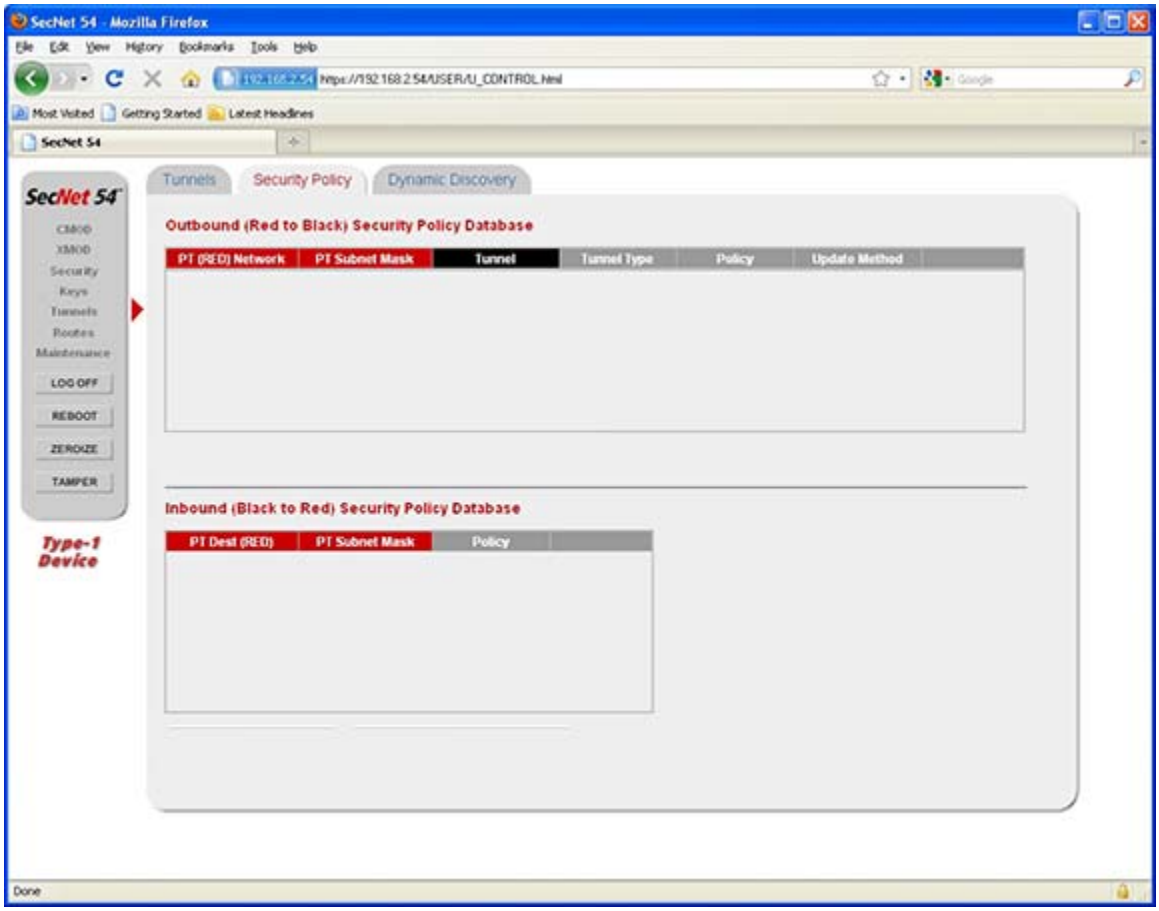
expires (i.e., the current MTEK expires) the Next Role will become N/A and the Current Role will become what the Next Role was.

j. (U//FOUO) TFS Settings - The default TFS settings for all tunnels or TFS settings that are specific to this tunnel. Refer to Section 3.2.7.2 for descriptions of the TFS settings.

3.2.9.1 (U) Viewing the Security Policy Configurations

(U//FOUO) The **Security Policy** tab selection displays Outbound (Red to Black) and Inbound (Black to Red) Security Policy Database tables as configured by the Administrator. Both tables are view only to the User.

UNCLASSIFIED//FOUO



UNCLASSIFIED//FOUO

(U) The Security Policy database tables contain the following information:

1. (U//FOUO) Outbound (Red to Black) Security Database:

   a. (U//FOUO) PT (Red) Network - The Plain Text (PT) destination (Red/classified) target that this device can reach using the associated tunnel.

   b. (U//FOUO) PT Subnet Mask - The Subnet Mask (PT) and bits reserved for identifying the subnet for the PT target node or network.

c. (U//FOUO) Tunnel - The IP address of the Cipher Text (CT) Black destination HAIPE® end-point (HAIPE® device on the other end of "this" tunnel). This field may show "Not Discovered" if a dynamic SPD entry was entered but the tunnel has not been established.

d. (U//FOUO) Tunnel Type - Indicates whether the tunnel is a statically defined or dynamically discovered tunnel type. "Static" indicates that a static (user-defined) SPD entry is associated with this tunnel. "Dynamic" indicates that the tunnel was dynamically created through the Dynamic Discovery process (refer to Section 3.2.9.3).

e. (U//FOUO) Policy - The security policy that is associated with the outbound Tunnel. The policies consist of Apply IPSec and Discard (i.e., Apply IPSec Processing and Discard Packet).

f. (U//FOUO) Update Method - This field applies to tunnels assigned FIREFLY key types. During the HAIPE® IKE negotiating, an update method is established. Update methods are as follows:

- (U//FOUO) MTEK - A new HAIPE® IKE negotiation is done every 24 hours on the FIREFLY SA entries to establish a new MTEK.
- (U//FOUO) MTEK/Update (ACCORDION) - an Accordion 3.0 update is done every 24 hours instead of a new HAIPE® IKE negotiation.

2. (U//FOUO) Inbound (Black to Red) Security Policy Database

a. (U//FOUO) PT Dest (RED) - The Plain Text Red Network IP address. The IP address for each source (classified) node with which this device can receive decrypted packets through established tunnels.

b. (U//FOUO) PT Subnet Mask - The source network Subnet Mask and bits reserved for identifying the subnet of the Red source node.

c. (U//FOUO) Policy - The Policy selection determines if the security policy will be associated with the inbound tunnel. The policy is either allowed or discarded.

3.2.9.2 (U) Enabling and Disabling Tunnel Connectivity

(U//FOUO) The tunnel's connectivity can be enabled or disabled from the **Tunnel Configuration** status page (Section 3.2.9). Specifics regarding static PPK tunnels and static and Dynamic HAIPE® IKE tunnels are as follows:

a. (U//FOUO) Static PPK Tunnels - When static PPK tunnels are created, they are automatically enabled. However, they can be manually disabled by selecting the **Disable** button associated with the tunnel. The **Disable** button then changes to **Enable**, the tunnel's Connectivity (Conn) Status displays "Disabled", and traffic cannot be sent or received. To re-enable the tunnel the **Enable** button is selected, the button name changes to **Disable**, the tunnel's Connectivity (Conn) Status displays "Enabled", and traffic can be sent or received.

b. (U//FOUO) Static and Dynamic Discovery HAIPE® IKE Tunnels

- (U//FOUO) Establish Static HAIPE® IKE tunnels - Selecting the **Connect** button associated with a HAIPE® IKE tunnel initiates the process of establishing a tunnel. The HAIPE®

IKE Tunnel's Connectivity (Conn) Status displays "Connected" when the HAIPE® IKE process has been completed, and the **Connect** button changes to **Disconnect**.

- (U//FOUO) Establish Dynamic Discovery HAIPE® IKE tunnels - The tunnel is automatically established when traffic is sent to an IP address that matches an SPD associated with Dynamic Discovery and Dynamic HAIPE® IKE tunnels.
- (U//FOUO) Establish all HAIPE® IKE tunnels - Selecting the **Establish All FIREFLY Tunnels** button initiates the discovery process for all HAIPE® IKE tunnels created. However, if communications have not been enabled (i.e., XMOD enabled. Refer to Section 3.2.6.1), the following message displays:

UNCLASSIFIED//FOUO

UNCLASSIFIED//FOUO

(U//FOUO) When the **Establish All FIREFLY Tunnels** button is selected after communication has been enabled, a message displays indicating that only FIREFLY tunnels that are disconnected will be enabled. Selecting the **OK** button from this message displays the following status message:

Please wait while your changes are applied...

(U//FOUO) Once HAIPE® IKE is in progress, the **Connect** button changes to **Cancel IKE** and the Connectivity (Conn) Status displays "IKE In Progress". While HAIPE® IKE is in progress, the HAIPE® IKE negotiation can be canceled by selecting the **Cancel IKE** button.

(U//FOUO) When communication errors are captured by SecNet 54®, as the tunnel is enabling, a Details hyperlink appears in the appropriate column beside the word "Error" as illustrated in the following figure. Selecting the Details hyperlink displays the error description (e.g., the PPK Chain not having an active PPK).

UNCLASSIFIED//FOUO

UNCLASSIFIED//FOUO

- (U//FOUO) Disconnect Static and Dynamic Discovery HAIPE® IKE Tunnels - When disconnecting HAIPE® IKE tunnels, selecting the **Disconnect** button associated with the tunnel disconnects the tunnel. A HAIPE® IKE tunnel Connectivity (Conn) Status displays "Disconnected" when the tunnel is no longer connected to the destination to the destination HAIPE® device.

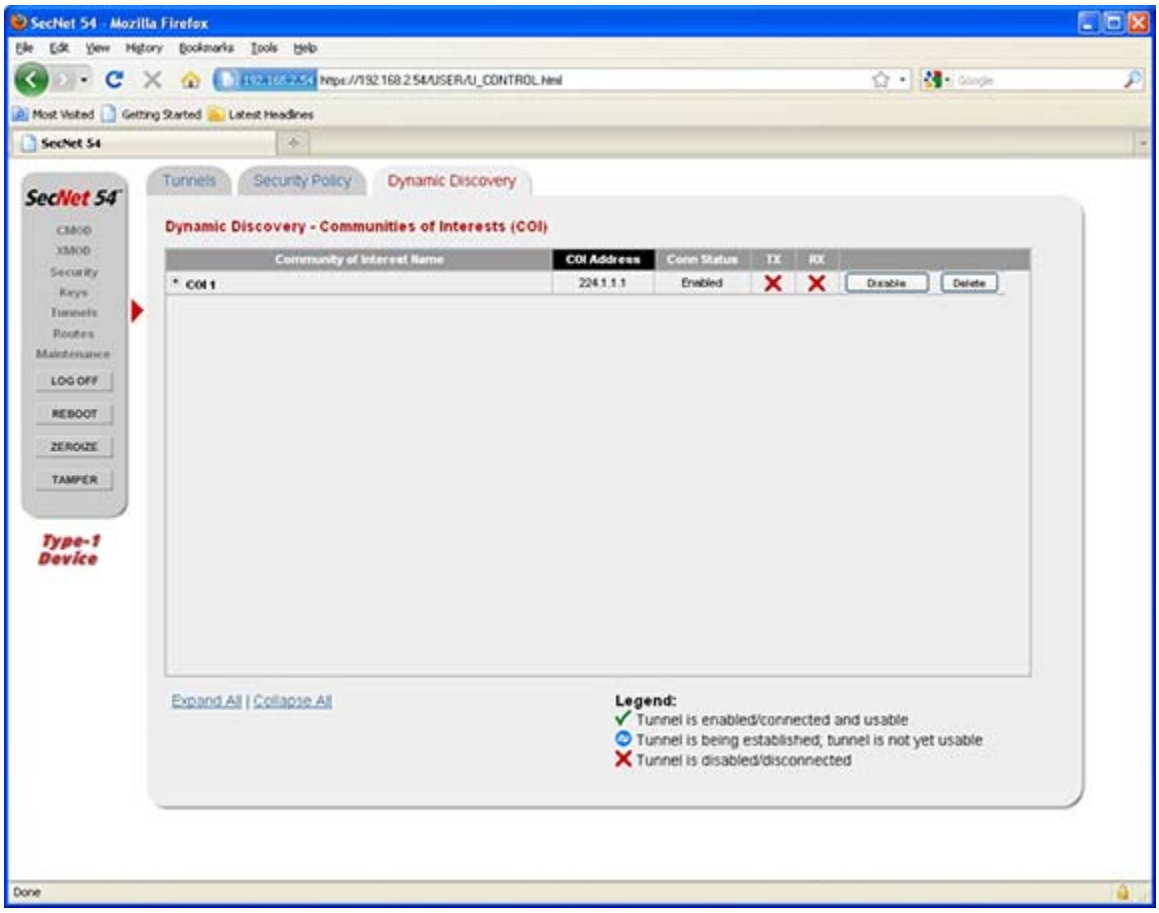
3.2.9.3 (U) Viewing Dynamic Discovery COIs

(U//FOUO) Dynamic Discovery is the process by which the SecNet 54® device fronting an originating host locates the corresponding HAIPE® device that is fronting the target host to which traffic is intended, even if the address of the corresponding target HAIPE® is unknown. The discovery process is used by an originating SecNet 54® device to determine the Black CT address of a target HAIPE® device. The originating device is fronting an originating Red host that is sourcing packets through that SecNet 54® device. The target HAIPE® device is fronting the Red host for which the packets from the originating host are destined. Both HAIPE® devices must be part of the same COI.

(U//FOUO) A COI consists of a Dynamic Discovery Multicast PPK tunnel and a specific PPK Chain to be used for the Dynamic Discovery process. All devices within the COI are loaded with the same PPKs. The COI is used during the Dynamic Discovery process to locate target nodes and their fronting HAIPEs. After Dynamic Discovery completes, HAIPE® IKE is used to create tunnels. The SecNet 54® device supports up to 64 COIs.

(U//FOUO) The **Dynamic Discovery** tab selection displays Dynamic Discovery COIs as configured by the Administrator. The COIs are view only to Users.

UNCLASSIFIED//FOUO



UNCLASSIFIED//FOUO

(U//FOUO) The **Dynamic Discovery - Communities of Interests (COI)** status page displays the COI Name and COI Address as well as the tunnel Connectivity Status. Components unique to the COI table are as follows:

a. (U//FOUO) Community of Interest Name - The name assigned by the Administrator when defining the COI.

b. (U//FOUO) COI Address - The Multicast IP address of the group of HAIPE® devices. Each COI group member has the identical Multicast IP address.

c. (U//FOUO) Conn Status - The COI's Connectivity Status. The status indicates if the COI's connectivity is enabled and ready for use or disabled. It is associated with the tunnel's ability to transmit (TX) or receive (RX) traffic.

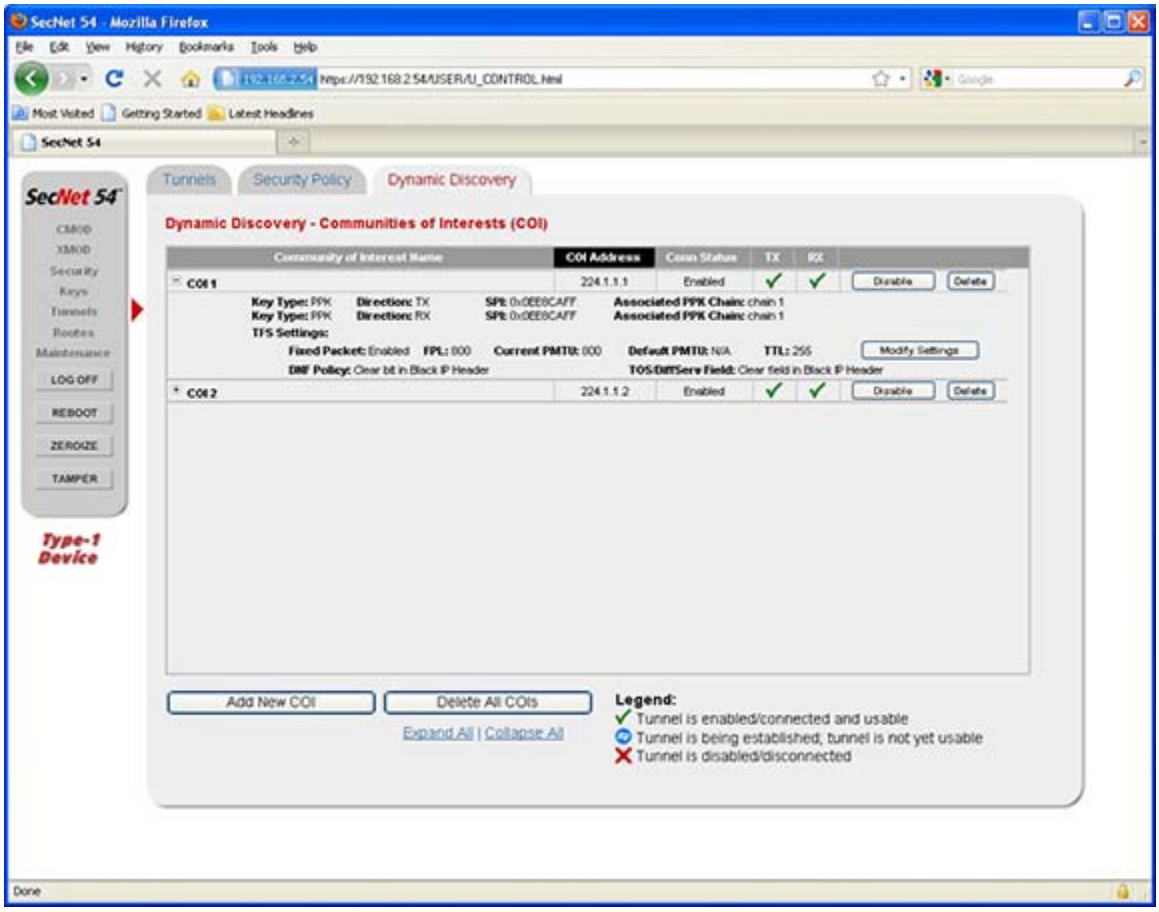
d. (U//FOUO) TX/RX - The TX and RX columns indicate the connection status and display the following symbols as visual indications:

(U//FOUO) When displayed in one or both columns, this green symbol indicates that information may be transmitted or received to/from the receiving host. The COI is enabled.

(U//FOUO) When displayed in the either columns, as a red symbol, this indicates that the COI has been manually disabled and is not available.

(U//FOUO) Expanding the COI name (i.e., selecting the plus (+) symbol) displays additional data associated with the COI. Fields associated with the COI are displayed in the following figure and described in the following listing.

UNCLASSIFIED//FOUO



UNCLASSIFIED//FOUO

a. (U//FOUO) Key Type - The Key Type is PPK.

b. (U//FOUO) Direction - The COI routes traffic bi-directional (TX/RX). The COI is a Multicast tunnel traffic type.

c. (U//FOUO) TX SPI/RX SPI - The SPI is a 32-bit value used to identify the SA at the receiving HAIPE® device. The SPI for the COI is developed during the PPK association setup. It is only associated with a FIREFLY tunnel if the tunnel is established with the destination HAIPE® device. Prior to the PPK for the COI expiring, a changeover notification is displayed on the **Current Status** page as an alert (Section 3.2.5.1), the alert is logged in the audit log, and a second SPI value displays (a 55 minute time-frame) for both TX and RX, if both are applicable. The word “Next” also displays beside the connectivity direction of the newly acquired SPI. During changeover, data may be received on either the Current or the Next SPIs. However, data that is transmitted is always done on the Next SPI. Upon exiting the changeover window, the Current SPIs expire and the Next SPIs are used to receive and transmit all data

d. (U//FOUO) Associated PPK Chain - The PPK Chain selected when configuring the COI.

e. (U//FOUO) TFS Settings - The TFS settings may be specific to this COI or the default TFS settings for all COIs. Refer to Section 3.2.7.2 for descriptions of the TFS settings

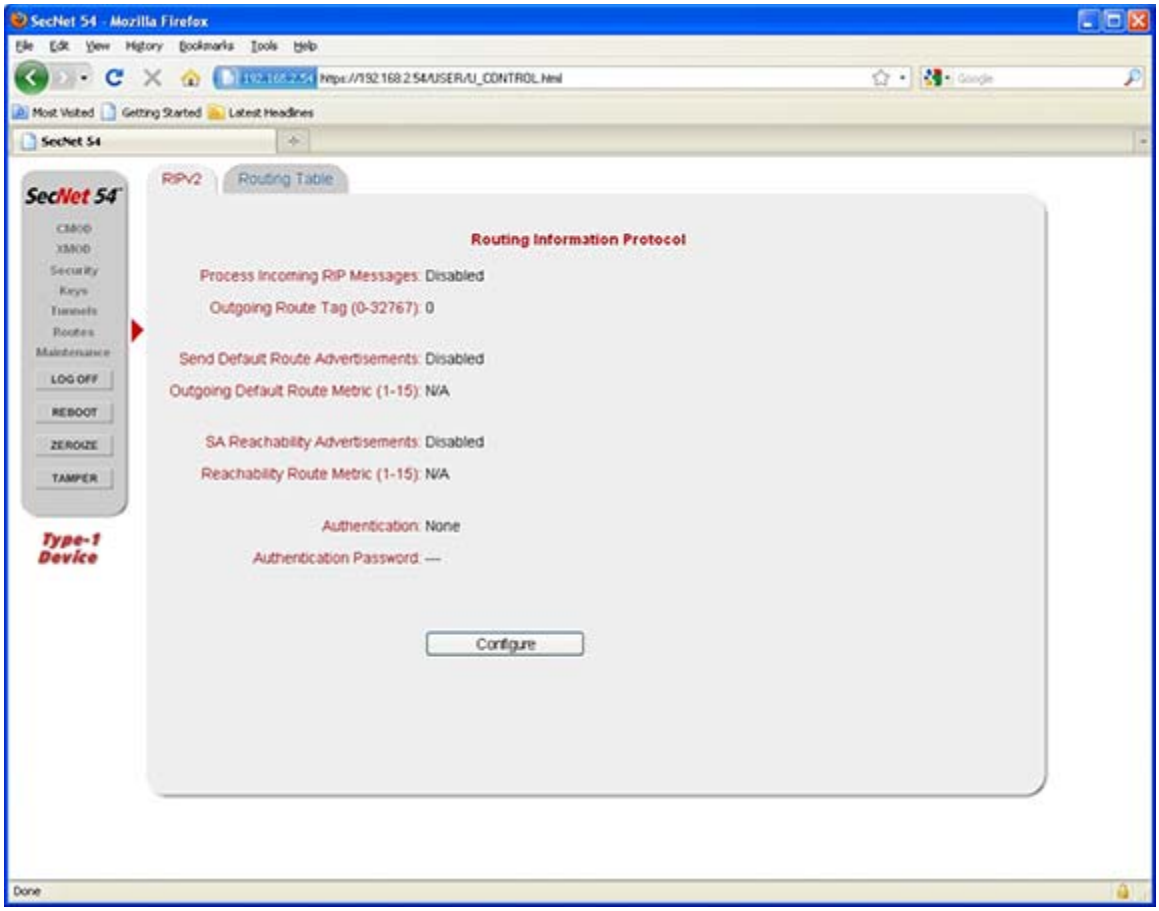
3.2.9.4 (U) Enabling and Disabling Dynamic Discovery COI Tunnel Communications

(U//FOUO) COIs are automatically enabled when configured by the Administrator via the **Dynamic Discovery - COI** status page (refer to Section 3.2.9.3). However COIs can be manually disabled by selecting the **Disable** button. When COIs are disabled, the Conn Status field displays Disabled and the button changes to **Enable**. COIs are re-enabled by selecting the **Enable** button associated with the COI. When the COI is re-enabled, the Conn Status displays Enabled and the button changes to **Disable**. Refer to the table in Section 3.2.9.3 for additional information about the connectivity status icons and their color coding.

3.2.10 (U) Viewing Red-side Routes

(U//FOUO) Configuring RIPv2 is an Administrator login privilege. Users have only view only privileges. The **Routes** menu option displays the RIPv2 configuration status and the Red Routing Table. The Red-side routing accommodates multiple routers on a Red network. RIP uses broadcast technology where gateways broadcast their routing tables to the other gateways in the network and can flood a network with RIP messages when a system malfunctions. RIP obtains information about all the destinations in the system to which gateways belong. The **RIPv2** tab displays the **RIPv2 Status** page.

UNCLASSIFIED//FOUO



UNCLASSIFIED//FOUO

(U//FOUO) The following is a listing and description of RIPv2 settings:

a. (U//FOUO) Process Incoming RIP Messages - Enable or disable the capability to allow the SecNet 54® device to list for RIPv2 messages from a router on the local PT link and use the information to populate the Local Enclave Prefix Table.

b. (U//FOUO) Send Default Route Advertisements - Enable or diable sending (broadcasting) RIPv2 messages with the default route.

c. (U//FOUO) SA Reachability Advertisements - Enable or disable the capability of the SecNet 54® device to allow advertisement from its PT interface.

d. (U//FOUO) Outgoing Default Route Metric - Allow the configuration of the metric (hop count) from 1 to 15 that is advertised with the RIPv2 default route.

e. (U//FOUO) Outgoing Route Tag - The Route Tag field is an attribute assigned to a route which must be preserved and readvertised with a route. The intended use of the Route Tag is to provide a method of separating "internal" RIP routes (routes for networks within the RIP routing domain) from "external" RIP routes, which may have been imported from an Exterior Gateway Protocol or another Interior Gateway Protocol. A value of 0 is used in this field if the tag is not used.

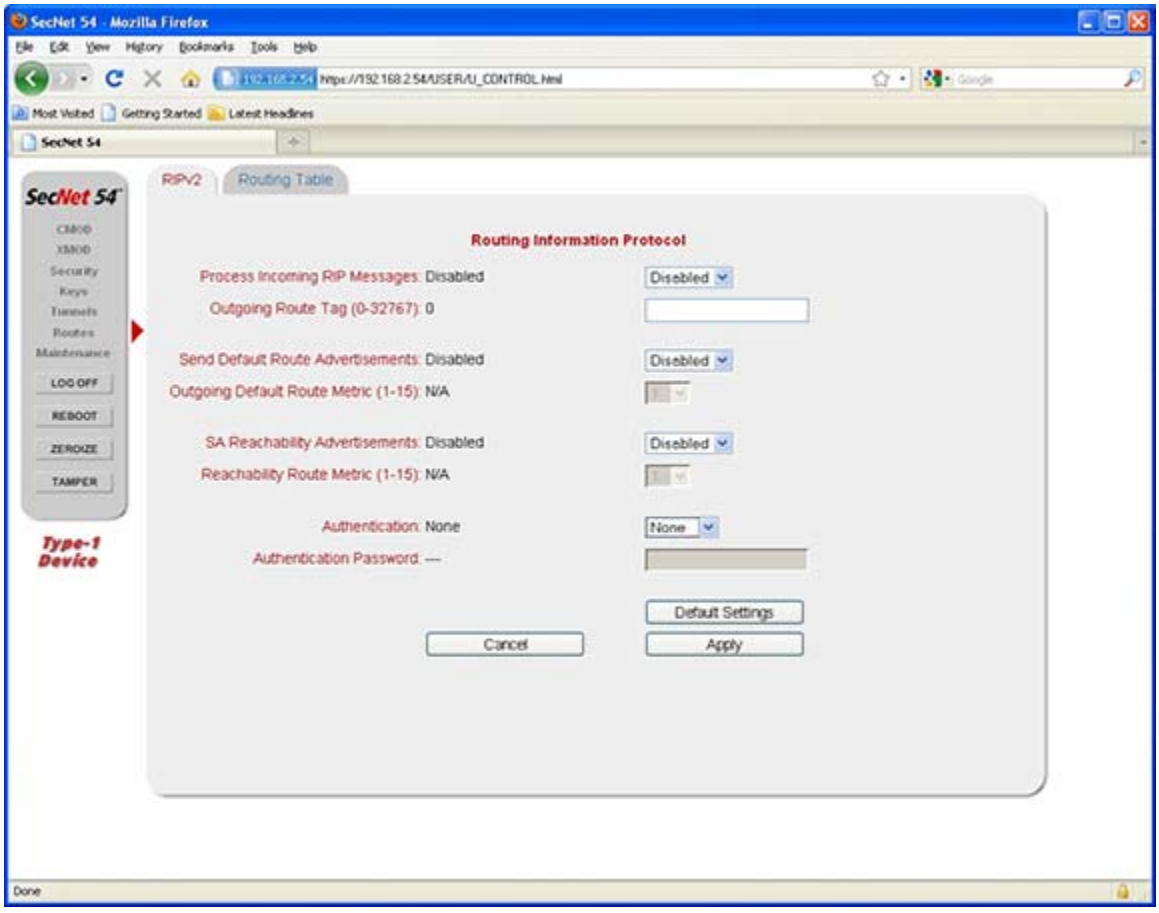
f. (U//FOUO) Authentication:

- None - No authentication is the default setting.
- Simple - Sends a password in the clear on the Red network.
- Message-Digest 5 (MD5) Authentication - A cryptographic hash function with a 128-bit hash value.

g. (U//FOUO) Authentication Password - The encrypted password for routing updates.

(U//FOUO) The **Routing Table** tab selection displays the **Red Routing Table - Local Enclave Prefix Table**. The auto entries are all Outbound SPD entries that are assigned an active/enabled SA as a table entry.

UNCLASSIFIED//FOUO



UNCLASSIFIED//FOUO

The Source column indicates if an entry is automatically generated (Auto), generated by RIP, or manually added by the Administrator. Manual routes are only removable by the Administrator. Auto and RIP entries are removed at the end of their route timeout period.

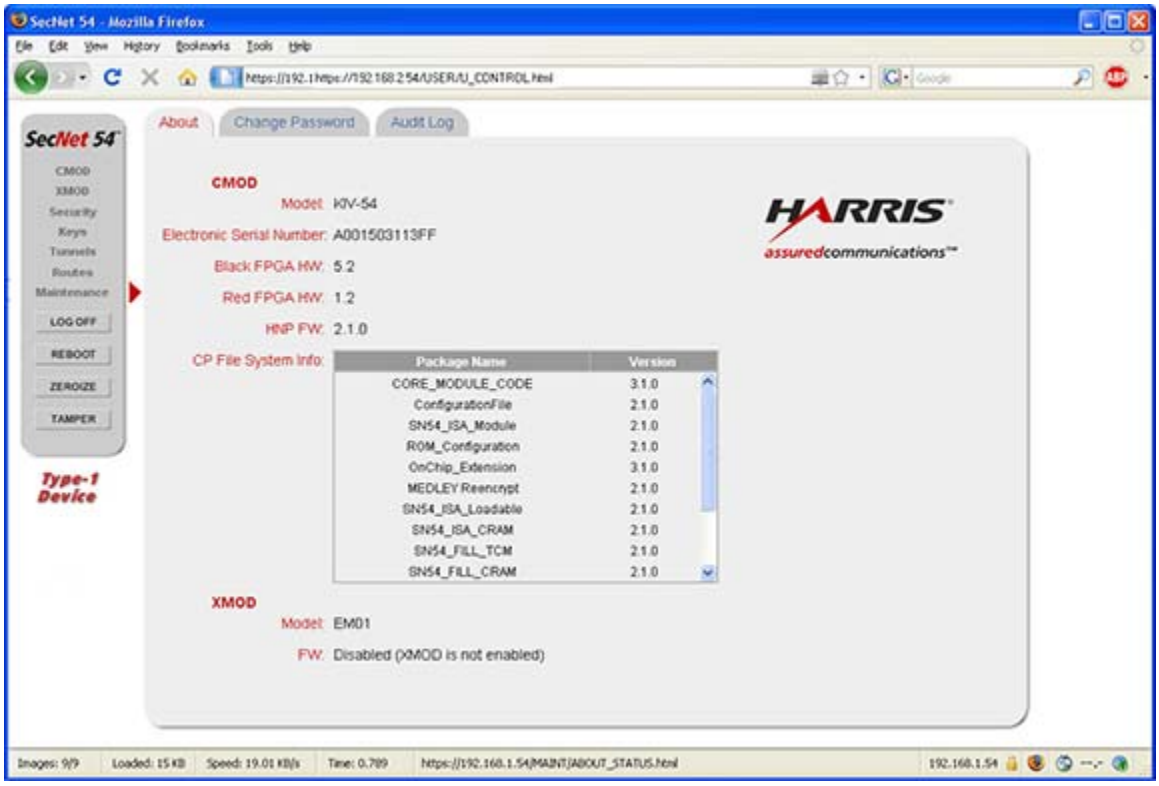
3.2.11 (U) Maintenance Operations

(U//FOUO) Selecting the **Maintenance** menu option allows the User or Administrator to view information about the CMOD and XMOD firmware (FW), CMOD HW (hardware), manage passwords, and manage the SecNet 54® Audit log.

3.2.11.1 (U) Viewing the SecNet 54® Firmware and Hardware Information

(U//FOUO) The **About** page is a status page that displays the CMOD Model number and the version numbers for all software and firmware that is running on the CMOD and the XMOD (if attached).

UNCLASSIFIED//FOUO



UNCLASSIFIED//FOUO

(U//FOUO) The **XMOD** status area indicates a “Disabled” state in all the data fields when the XMOD is not attached. When the XMOD is attached but not enabled, the Model data field indicates the type of XMOD and the FW data field indicates that it is not enabled. The following table describes information displayed on the **About** status page.

UNCLASSIFIED//FOUO

Module Components	Description
CMOD	This section lists information associated with the Cryptographic Module (i.e., CMOD).
Model	This is the Model number of the CMOD.
Electronic Serial Number	This is the Electronic Serial Number of the CMOD.
Black FPGA HW	This is the version number of the Black Field Programmable Gate Array (FPGA).
Red FPGA HW	This is the version number of the Red FPGA.
HNP FW	This is the FW version number of the FW loaded on the Host Network Processor (HNP) in the CMOD. The HNP FW handles and routes traffic, commands and controls other components in the device, and provides the external interfaces for discovery and management of the device.
CP File System Info	This table indicates the Cryptographic Processor (CP) software package name and version number that is on this device. The CP software package is the directory containing the CMOD software components.
XMOD	This section lists information associated with the attached External Module (i.e., XMOD).
Model	This is the model number of the XMOD attached to the cryptographic module.
FW	This is the Firmware (FW) version number of the FW loaded on the attached XMOD.

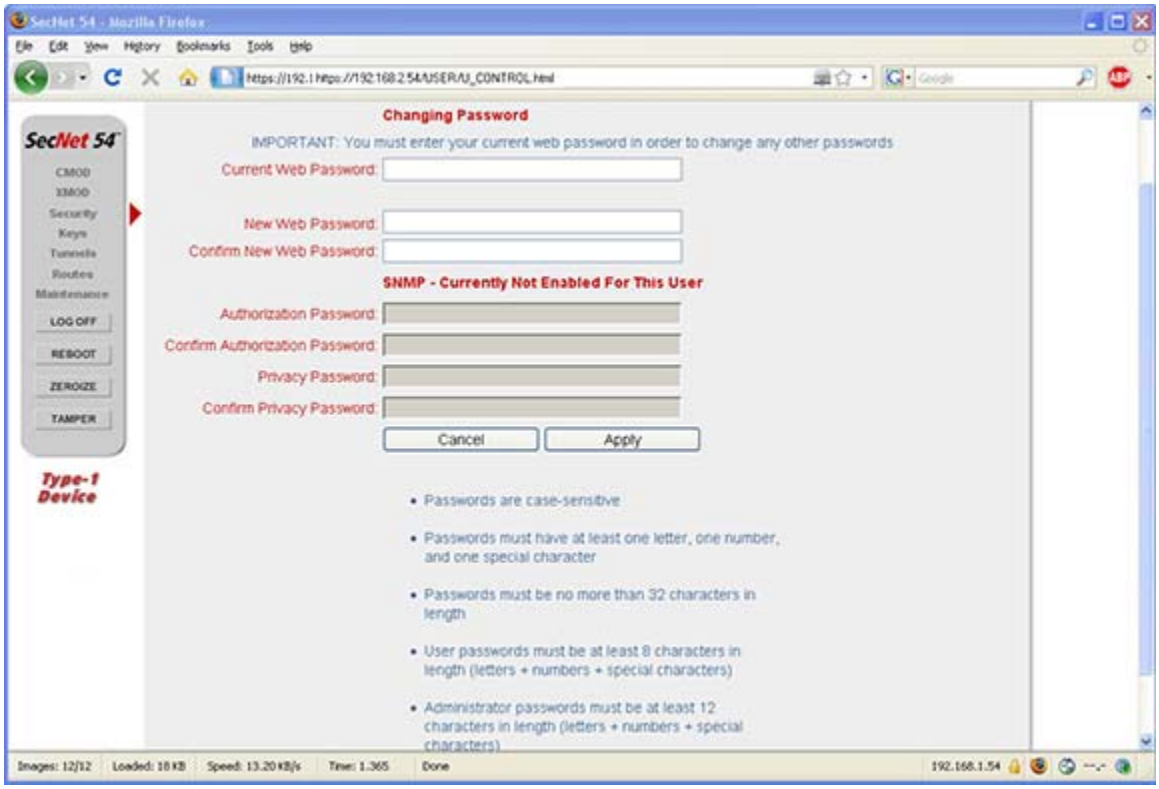
UNCLASSIFIED//FOUO

3.2.11.2 (U) Changing the User Password

(U//FOUO) The **Change Password** page allows a User to change their own password. The following User Password criteria apply.

- (U//FOUO) At least eight (8) characters
- (U//FOUO) Maximum of thirty-two (32) characters
- (U//FOUO) At least one (1) letter a-z, A-Z)
- (U//FOUO) At least one (1) number (0-9)
- (U//FOUO) At least one (1) special character (*,_,-,#,etc.) (The following are not valid values: double quotes, single quote, less than, greater than, and ampersand.)
- (U//FOUO) Cannot be identical to the Username

UNCLASSIFIED//FOUO

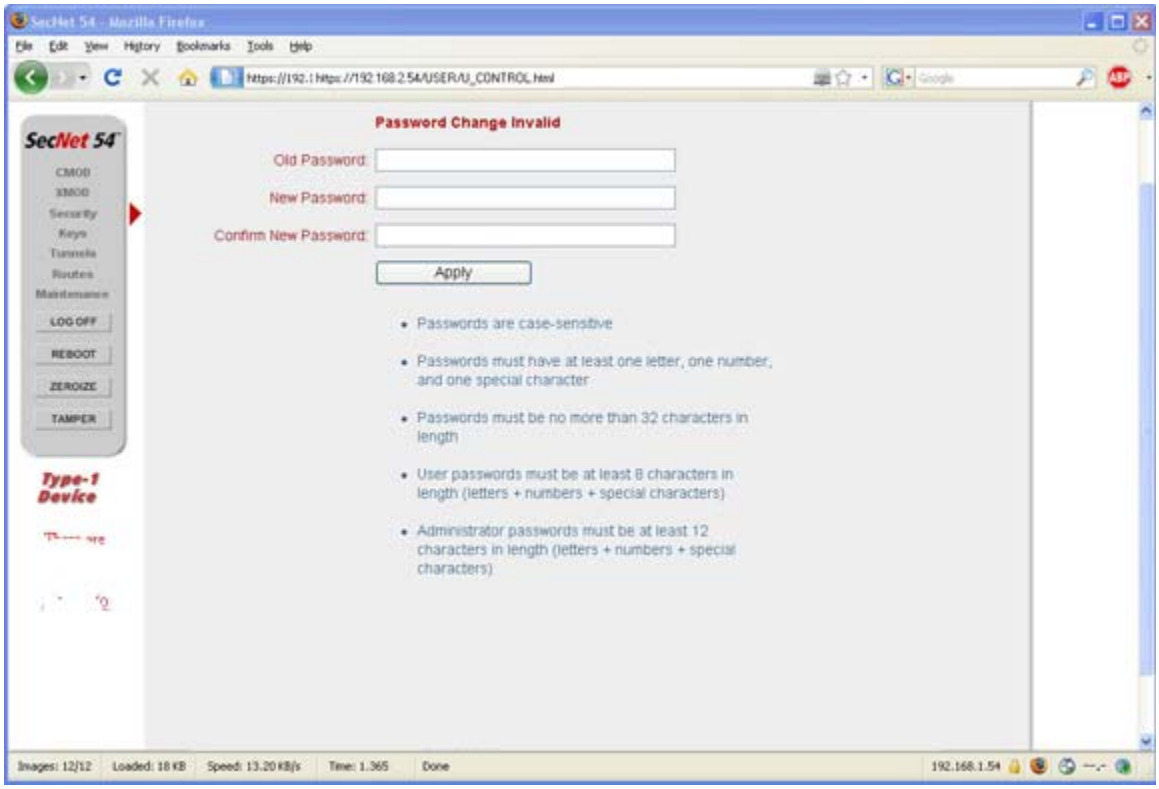


UNCLASSIFIED//FOUO

(U//FOUO) The User changes the password by entering values for the Old Password and New Password, and then confirming the New Password. The **Apply** button selection initiates the change.

(U//FOUO) When the New Password is validated, the page displays **Password Change Successful**. If any of the information is rejected, the **Password Change Invalid** page is displayed as shown below.

UNCLASSIFIED//FOUO

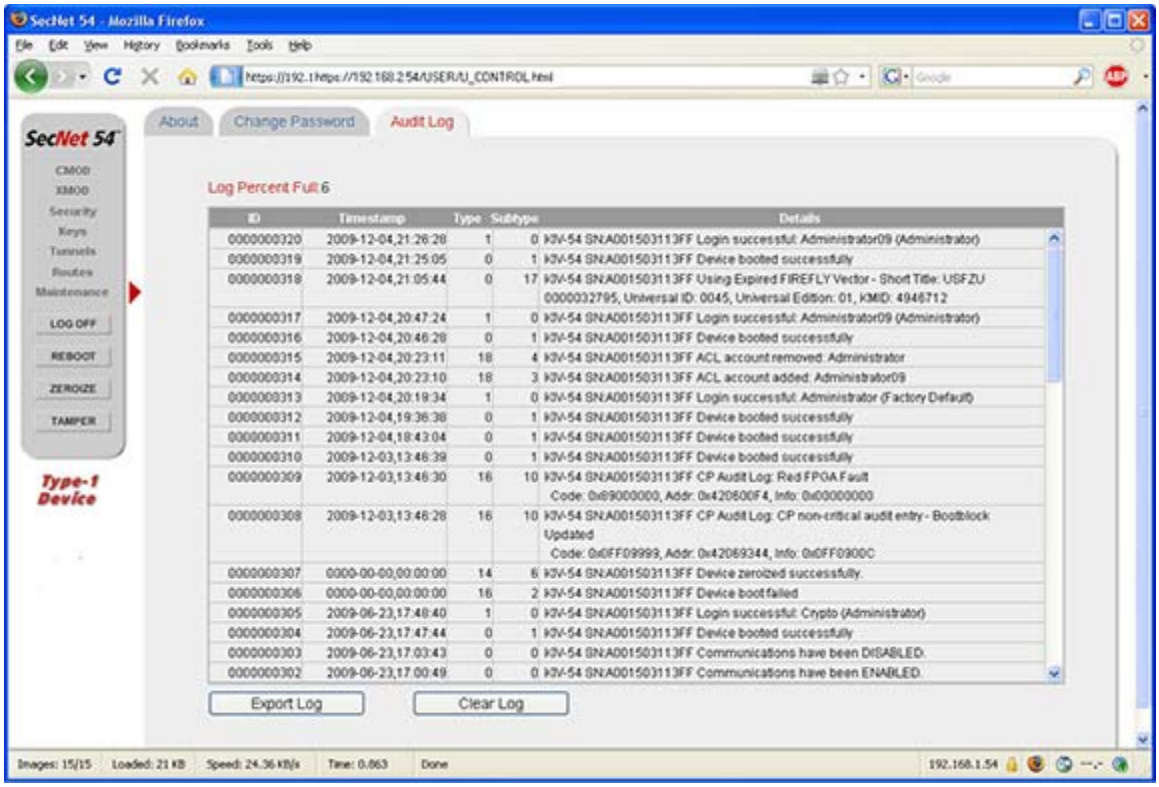


UNCLASSIFIED//FOUO

3.2.11.3 (U) Managing the SecNet 54® Audit Log

(U//FOUO) The **Audit Log** status page displays the SecNet 54® auditable events that have been captured by the SecNet 54® device and stored in the audit log. Although all auditable events are captured by the SecNet 54® device, only those events viewable with User authentication are viewable to a User. Auditable events that are not visible to a User include, but are not limited to, auditable events containing specific username information. In addition to viewing the auditable events in the status window, the User can also export the auditable events to a text file.

UNCLASSIFIED//FOUO



UNCLASSIFIED//FOUO

(U//FOUO) The **Audit Log** status page displays current and historical events in reversed chronological order with the most recent events visible. In the upper left-hand corner of the page is an indication (in percentages) of how full the log is. A scroll bar becomes available when the number of events exceed the viewable area on the status page. Included on the status page are columns displaying the following information:

a. (U//FOUO) ID - Unique identification number assigned to the event.

b. (U//FOUO) Timestamp - Date and time the event occurred. The Date is indicated as year-month-day and the time is indicated as hours:minutes:seconds.

c. (U//FOUO) Type - Type of audit event as defined by the HAIPE_ENTERPRISE_MIB. Contact the Administrator for additional information about the HAIPE® event types and values.

d. (U//FOUO) Subtype - SecNet 54® events that further breaks down the HAIPE® event types. Contact the Administrator for additional information about the SecNet 54® event subtypes and values.

e. (U//FOUO) Details - Event description that includes the device name and serial number.

NOTE

(U//FOUO) When the SecNet 54® is rebooted or powered off by the Power Switch, the log data is saved. However, disconnecting the power cord prior to powering down the device may corrupt the audit log as well as the configuration information if the data is being written at the time power is removed.

3-2.11.3.1 (U) Critical and Non-Critical Auditable Events

(U//FOUO) Auditable events are categorized as critical or non-critical. Critical events are of high priority and consist of security related events. The non-critical events are of a lower priority and are general operational and status events. Listed below are types of critical events that are seen by the user.

- (U//FOUO) Successful Startup
- (U//FOUO) Failed Trusted Boot
- (U//FOUO) Device Zeroized (Logged when the event occurs while power is on. The event is displayed the next time the device is powered up.)
- (U//FOUO) Alarm Condition
- (U//FOUO) Packet Failed Authentication Trailer
- (U//FOUO) Packet Sequence Number (PSEQN) Error
- (U//FOUO) Expired PPK Used
- (U//FOUO) Expired FIREFLY/Enhanced FIREFLY Vector Used
- (U//FOUO) Bad Sierra Crypto Processor Command Interface (SCPCI) Checksum
- (U//FOUO) SPD Lookup Failure
- (U//FOUO) Commanded Zeroize Failure

(U//FOUO) Listed below are types of non-critical events:

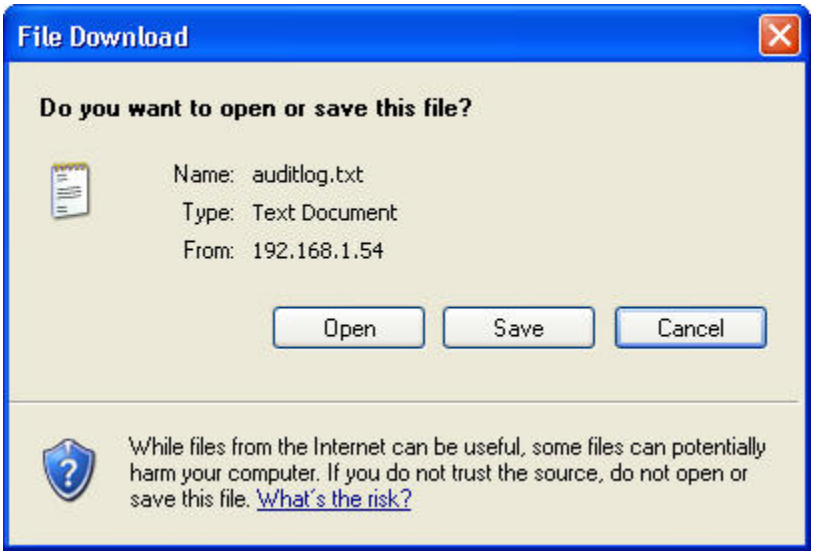
- (U//FOUO) Communication Enabled
- (U//FOUO) Communication Disabled
- (U//FOUO) IKE Negotiation Failure
- (U//FOUO) Tunnel Disconnected

3-2.11.3.2 (U) Exporting the Audit Log

(U//FOUO) The audit log stores up to 1000 events before overwriting the older ones. To prevent data loss, the User can download the audit log to a text file when the audit log nears a 100 percent capacity. When the log reaches 100 percent, the oldest entry is overwritten each time a critical auditable event occurs. This ensures that the active audit log always contains the most current data. Non-critical auditable events are treated differently when the audit log is full; they are not recorded until the audit log is cleared. Clearing the audit log is an administrative function. A full audit log does not interfere with the functionality of the SecNet 54® device.

(U//FOUO) The audit is exported in a text file format. Selecting the **Export Log** button displays the **File Download** window.

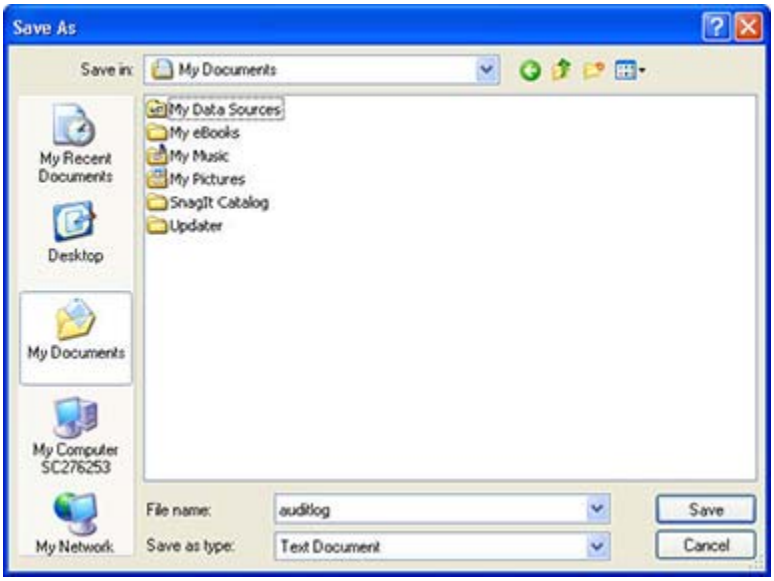
UNCLASSIFIED//FOUO



UNCLASSIFIED//FOUO

(U) Selecting the **Open** button displays the log without saving. Selecting the **Save** button initiates the export process. The **Cancel** button selection removes the window without saving the log. The **Save** button selection displays the **Save As** window.

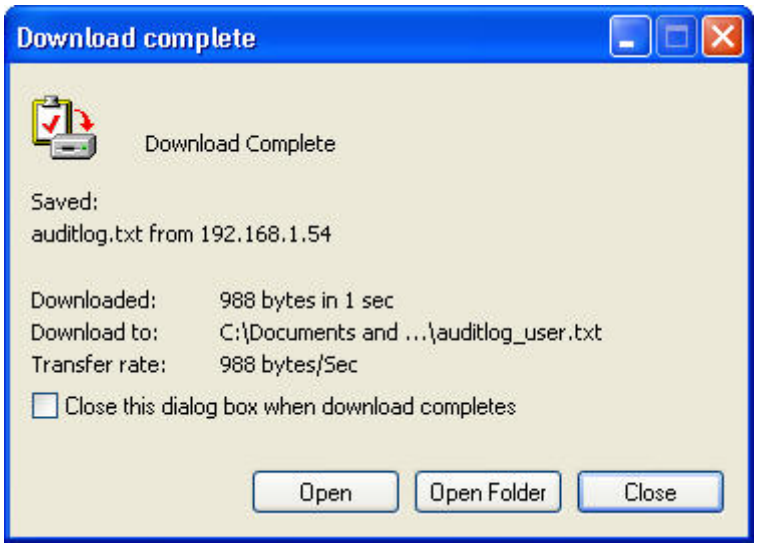
UNCLASSIFIED//FOUO



UNCLASSIFIED//FOUO

(U) Selecting the drop-down arrow for the “Save in” field (located at the top of the window) displays drives and folders to browse for an appropriate location. When the file name is edited in the “File name” data entry field (if appropriate), the **Save** button selection removes the **Save As** window. The **Download complete** window may display once the **Save As** window is closed, depending on the Internet browser’s settings for **Download** status windows.

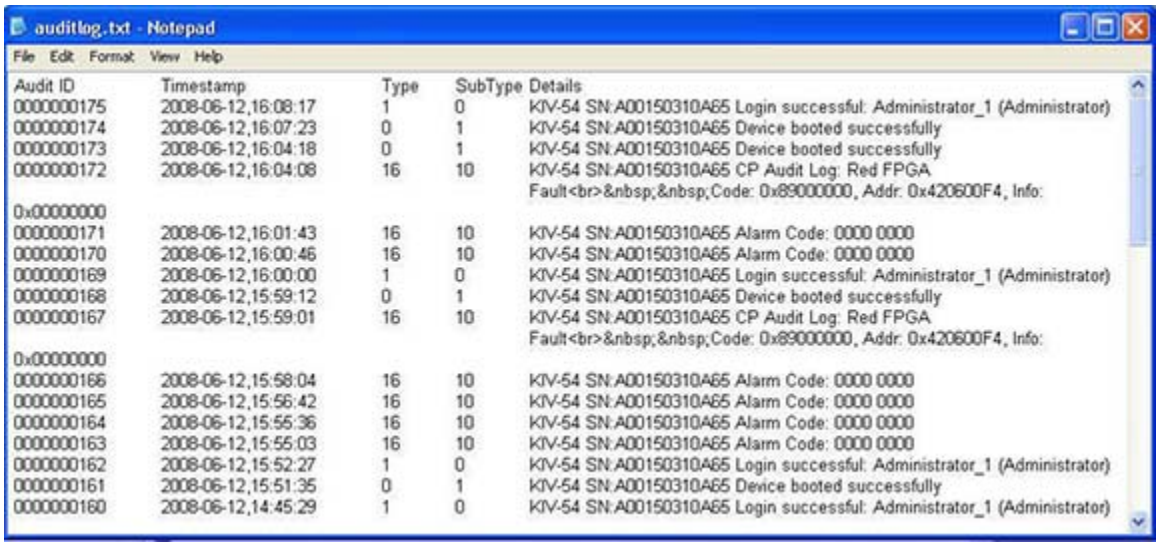
UNCLASSIFIED//FOUO



UNCLASSIFIED//FOUO

(U//FOUO) The **Open** button selection displays the saved text file and the **Close** button selection removes the window. The following figure is an example of the audit log in a text file format.

UNCLASSIFIED//FOUO



Audit ID	Timestamp	Type	SubType	Details
0000000175	2008-06-12,16:08:17	1	0	KIV-54 SN:A00150310A65 Login successful: Administrator_1 (Administrator)
0000000174	2008-06-12,16:07:23	0	1	KIV-54 SN:A00150310A65 Device booted successfully
0000000173	2008-06-12,16:04:18	0	1	KIV-54 SN:A00150310A65 Device booted successfully
0000000172	2008-06-12,16:04:08	16	10	KIV-54 SN:A00150310A65 CP Audit Log: Red FPGA Fault Code: 0x89000000, Addr: 0x420600F4, Info: 0x00000000
0000000171	2008-06-12,16:01:43	16	10	KIV-54 SN:A00150310A65 Alarm Code: 0000 0000
0000000170	2008-06-12,16:00:46	16	10	KIV-54 SN:A00150310A65 Alarm Code: 0000 0000
0000000169	2008-06-12,16:00:00	1	0	KIV-54 SN:A00150310A65 Login successful: Administrator_1 (Administrator)
0000000168	2008-06-12,15:59:12	0	1	KIV-54 SN:A00150310A65 Device booted successfully
0000000167	2008-06-12,15:59:01	16	10	KIV-54 SN:A00150310A65 CP Audit Log: Red FPGA Fault Code: 0x89000000, Addr: 0x420600F4, Info: 0x00000000
0000000166	2008-06-12,15:58:04	16	10	KIV-54 SN:A00150310A65 Alarm Code: 0000 0000
0000000165	2008-06-12,15:56:42	16	10	KIV-54 SN:A00150310A65 Alarm Code: 0000 0000
0000000164	2008-06-12,15:55:36	16	10	KIV-54 SN:A00150310A65 Alarm Code: 0000 0000
0000000163	2008-06-12,15:55:03	16	10	KIV-54 SN:A00150310A65 Alarm Code: 0000 0000
0000000162	2008-06-12,15:52:27	1	0	KIV-54 SN:A00150310A65 Login successful: Administrator_1 (Administrator)
0000000161	2008-06-12,15:51:35	0	1	KIV-54 SN:A00150310A65 Device booted successfully
0000000160	2008-06-12,14:45:29	1	0	KIV-54 SN:A00150310A65 Login successful: Administrator_1 (Administrator)

UNCLASSIFIED//FOUO

3.2.12 (U) Logging Out of the Configuration Web Pages

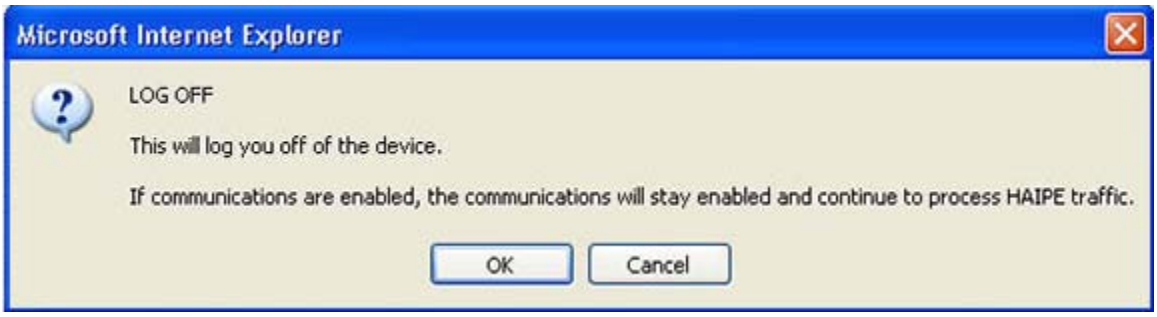
(U//FOUO) The **LOG OFF** option button (located on the main menu bar) is used to initiate the log out process from the configuration Web pages. It is always available during active login sessions, and it does not break the Ethernet connection or disable the device. The **LOG OFF** button should be used to close the Web browser configuration pages, not the Web browser close button located in the upper right hand corner (refer to Section 3.2.3).

NOTE

(U//FOUO) Closing the Web browser without using the **LOG OFF** button causes the Login Session to remain active until the 10-minute inactive time-out takes effect. This delays the ability to log into the device using a different IP Address. However, the device may be logged into using the same IP Address prior to the time-out period.

(U//FOUO) The **LOG OFF** button selection initiates the log out process and displays the following **LOG OFF** browser window:

UNCLASSIFIED//FOUO



UNCLASSIFIED//FOUO

(U//FOUO) Confirming the log off request results in the display of a **Session Closed** page in the Web browser window. Canceling the log off request removes the **LOG OFF** window and the session remains active.

3.2.13 (U) Rebooting the KIV-54RM01

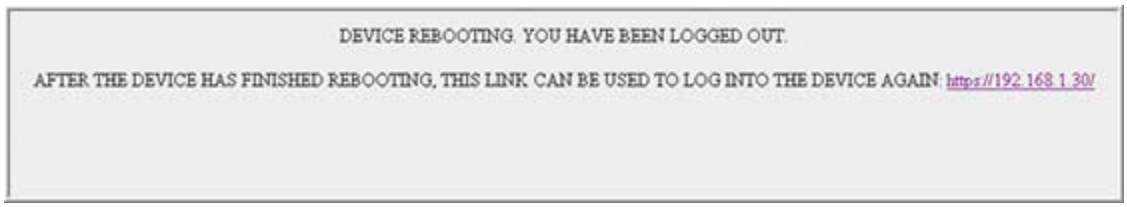
(U//FOUO) The **REBOOT** option button (located on the menu bar) is used to restart the device. The **REBOOT** button is always available during active Login Sessions. The **REBOOT** button selection displays the following confirmation window:

UNCLASSIFED//FOUO

UNCLASSIFIED//FOUO

(U//FOUO) Confirming the reboot displays the **DEVICE REBOOTING** page and logs out the User. The device is disconnected and then restarted. The **Cancel** button selection negates the command and the **REBOOT** confirmation window closes. Reboot has the same affect as cycling the power off then back on.

UNCLASSIFIED//FOUO



UNCLASSIFIED//FOUO

3.2.14 (U) Zeroizing the KIV-54

(U//FOUO) The **ZEROIZE** option button (located on the menu bar) is used to erase all encryption keys, key information (excluding Alternate and Base P^3 dePAC Moduli), and tunnels, disabling communication. The ACL is cleared and set back to the default username and password as the only entries. It does not clear the Red or Black Network settings.

(U//FOUO) The **ZEROIZE** button selection displays the following **ZEROIZE** Web browser confirmation window.

UNCLASSIFIED//FOUO

UNCLASSIFIED//FOUO

(U//FOUO) Confirming the zeroize (i.e., selecting the **OK** button) displays the following page:

UNCLASSIFIED//FOUO

UNCLASSIFIED//FOUO

(U//FOUO) The **Cancel** button selection negates the command and the **ZEROIZE** Web browser confirmation window closes.

This page intentionally left blank.

Chapter 4

(U) KIV-54RM01 OPERATIONS

4.1 (U) CHAPTER CONTENTS

(U) This chapter contains the following information:

- (U) KIV-54RM01 Setup and Configuration
- (U) Operating the KIV-54RM01 for Client Communications
- (U) Rebooting the KIV-54RM01
- (U) Zeroizing the KIV-54

4.2 (U) KIV-54RM01 USER SETUP AND CONFIGURATION

(U//FOUO) The KIV-54RM01 (or SecNet 54® device) must be set up and configured by the Administrator for use once it is received from the factory. After the administrative setup and configuration procedures are performed (i.e., added a User account, configured the KIV-54RM01, and configured the tunnels), it is recommended that the following User setup and configuration procedures are performed first in the order that they are listed in the following table.

UNCLASSIFIED//FOUO

Action	Reference
1. SecNet 54® SSL Certificate Installation into the default Web browser OR Customer-developed SSL Certificate Installation using the **Security** menu	Appendix G Sections 3-2.7.3.1 and 3-2.7.3.2
2. KIV-54 Power on	Section 2.3.1.3
3. Configuration Web pages login	Section 3.2.2
4. User password modification	Section 3.2.11.2
5. Device operating mode configuration	Section 3.2.6

UNCLASSIFIED//FOUO

4.3 (U) OPERATING THE KIV-54RM01 FOR CLIENT COMMUNICATIONS

(U//FOUO) After the Administrator and User KIV-54RM01 setup and configuration are complete, the KIV-54RM01 is ready for use. Perform the following procedure to operate the device for client communications. Refer to the referenced sections for additional information about the procedural steps.

UNCLASSIFIED//FOUO

Action	Reference
1. Set the KIV-54 power switch to the On position. Note that the radio remains off.	Section 2.3.1.3
2. Enter the device's IP address as the Uniform Resource Locator (URL) into the Web browser Address bar (or Location bar)	Section 3.2.2
3. Select **XMOD** from the menu bar.	Section 3.2.6
4. Enable the radio. This process can take up to one minute to complete.	Section 3.2.6.1

UNCLASSIFIED//FOUO

4.4 (U) REBOOTING THE KIV-54RM01

(U//FOUO) When a KIV-54RM01 has been rebooted, the User is logged out. The KIV-54RM01 is disconnected and then restarted. Perform the following procedure to reboot the KIV-54RM01. Refer to the referenced sections for additional information.

UNCLASSIFIED//FOUO

Action	Reference
1. Perform one of the following functions: • On the configuration Web page, select the **REBOOT** button from the menu bar. • Set the KIV-54RM01 power switch to the Off position and then set the power switch back to the On position.	Section 3.2.13 Section 2.3.1.3
2. After the KIV-54RM01 restarts, visually verify that its LINK LED illuminates green and steady.	Section 2.3.1.1

UNCLASSIFIED//FOUO

(U//FOUO) After the reboot process is complete, the User can log into the configuration Web pages (refer to Section 3.2.2.3) to view status or modify configurations.

4.5 (U) ZEROIZING THE KIV-54

(U//FOUO) The KIV-54 is zeroized from the configuration Web pages or from the KIV-54. This zeroize function erases all encryption keys, key information (excluding Base and Alternate P^3 dePAC Moduli), Access Control List (ACL), and tunnels, disabling communications. Perform the desired action to zeroize the KIV-54. Refer to the referenced sections for additional information.

UNCLASSIFIED//FOUO

Action	Reference
To zeroize a KIV-54 from the configuration Web pages: Select the **ZEROIZE** button on the menu bar and confirm the zeroize function.	Section 3.2.14
To zeroize the KIV-54 while power is off: Simultaneously press the Panic Zeroize buttons until the ALARM LED illuminates steady. **NOTE** Perform this operation in a panic situation only.	Section 2.3.1.2
To zeroize the KIV-54 while the power is on: 1. Simultaneously press the Panic Zeroize buttons until the ALARM LED flashes. 2. Wait approximately 15 seconds and turn the power off. The KIV-54 returns to the factory default state. 3. Power the device back on. It will take approximately 1 minute and 5 seconds to complete the boot-up process after a zeroize function. Although the PWR, LINK and FILL LEDs flash during the boot-up process, do not power down the device.	Section 2.3.1.2

UNCLASSIFIED//FOUO

Appendix A

(U) ACRONYMS, ABBREVIATIONS, AND GLOSSARY

(U) This appendix contains terms and definitions found in this SecNet 54® manual.

(U) 802.3	IEEE **802.3** is a comprehensive International Standard for Local Area Networks (LANs) employing Carrier Sense Multiple Access with Collision Detection (CSMA/CS) as the access method.
(U) 802.11	IEEE **802.11** Wireless Lan Standard

-A-

(U) AC	**A**lternating **C**urrent
(U//FOUO) ACL	**A**ccess **C**ontrol **L**ist
(U) Ad Hoc Network	The Nodes communicate directly with each other, without passing data through a central Access Point.
(U//FOUO) AES	**A**dvanced **E**ncryption **S**tandard
(U) AH	**A**uthentication **H**eader
(U) AP	**A**ccess **P**oint. A central node in an Infrastructure network.
(U) ASCII	**A**merican **S**tandard **C**ode for **I**nformation **I**nterchange. Text that is a code for representing English characters as numbers, with each letter assigned a number from 0 to 127.
(U//FOUO) Association	A connection between a station and an Access Point or between Ad Hoc Stations or Wireless Bridges. The connection (association) must occur before the device is allowed to communicate on the network.
(U) Audit Log	A group of recorded audit entries.
(U) Auditable Event	One of a defined list of situations whose occurrence is recorded by storing information about that occurrence.

-B-

(U) BATT	**B**attery
(U) Black Network	An unclassified (or nonsecure) network.
(U) Boot	To start and initialize the operating system on a computer or a device.

-C-

(U) CA	**C**ertification **A**uthority

(U) CBC-MAC	**C**ipher **B**lack **C**haining-**M**essage **A**uthentication **C**ode
(U//FOUO) CCI	**C**ontrolled **C**ryptographic **I**tem
(U) CCMP	**C**ounter-Mode/**C**BC-**M**AC **P**rotocol
(U) CD	**C**ompact **D**isc. A non-volatile optical data storage medium using the same physical format as audio compact discs and is readable by computers with Compact Disc-Read Only Memory (CD-ROM) drives.
(U) CIDR	**C**lassless **I**nter-**D**omain **R**outing. An IP addressing design that replaces the older networking system based on classes A, B, and C. Using CIDR, a single IP address can be used to designate many unique IP addresses.
(U//FOUO) CMOD	**C**ryptographic **Mod**ule. A KIV-54 that performs data encryption and decryption thereby rendering the data unintelligible to all but the intended receiver.
(U) CMOS	**C**omplementary-**M**etal-**O**xide-**S**emiconductor
(U//FOUO) COI	**C**ommunity **o**f **I**nterest. A group of HAIPE® devices with common key material and compatible IP addresses.
(U//FOUO) COMSEC	**Com**munications **Sec**urity. The protection of communications from exploitation by an adversary. This includes ensuring the security of crypto systems, preventing electronic emissions from various communications equipment, and physical protection of communications security equipment.
(U) COTS	**C**ommercial **O**ff-**t**he-**S**helf
(U//FOUO) CP	**C**ryptographic **P**rocessor
(U//FOUO) Critical Event	One of a defined subset of auditable events consisting of security related events.
(U) CSS	**C**ascading **S**tyle **S**heet. A stylesheet language used to describe the presentation of a document written in markup language.
(U) CT	**C**ipher **T**ext. Encrypted data that is unreadable until it has been converted into plain text (decrypted) with a key.

-D-

(U) dBi	**D**ecibels **o**ver **I**sotropic
(U) DC	**D**irect **C**urrent

(U) DES	**D**ata **E**ncryption **S**tandard. A cryptographic algorithm that is part of many standards.
(U) DH	**D**iffie-**H**ellman. A cryptographic key-exchange algorithm that is part of many standards.
(U) DHCP	**D**ynamic **H**ost **C**onfiguration **P**rotocol. A protocol for assigning dynamic IP addresses to nodes on a network (i.e., computers or other network devices). With dynamic addressing, a device can have a different IP address with each network connection, and with some system's a device's IP address can change while it is still connected. DHCP also supports a mix of static and dynamic IP addresses.
(U//FOUO) DMP	**D**evice **M**anagement **P**rotocol
(U) DNF	**D**o **N**ot **F**ragment
(U) DNS	**D**omain **N**ame **S**erver
(U) DSSS	**D**irect **S**equence **S**pread **S**pectrum
(U) DTD	**D**ata **T**ransfer **D**evice
(U//FOUO) Dynamic Discovery	A process by which a HAIPE® device fronting as an originating host (i.e., a Fronting HAIPE®) locates the corresponding HAIPE® device that is fronting the target host to which traffic is intended, even if the IP address of the corresponding target HAIPE® is unknown. The discovery process is dynamic and is used by an originating HAIPE® device to determine the Black CT address of a target HAIPE® device. The originating HAIPE® device is fronting an originating Red host that is sourcing packets through the HAIPE® device. The target HAIPE® device is fronting the Red host for which packets from the originating host are destined.
(U//FOUO) Dynamic Discovery IKE Tunnel	A tunnel that uses NSA Type-1 FIREFLY Vectors, where the HAIPE® device at each end of the a tunnel has the same vectors loaded, however, no specific tunnel has to be configured or established prior to use. This tunnel must be associated with a security policy, but the HAIPE® Dynamic Discovery process determines the proper tunnel end point IP addresses, and HAIPE® IKE negotiates the key to use. The Dynamic Discovery and HAIPE® IKE processes are initiated when a packet is received from the Red network that matches a security policy associated with a Dynamic Discovery HAIPE® IKE tunnel.

-E-

(U) EAP	**E**xtensible **A**uthentication **P**rotocol

(U//FOUO) EFF	**E**nhanced **F**IRE**F**LY
(U) EIRP	**E**ffective **I**sotropic **R**adiated **P**ower
(U//FOUO) EKMS	**E**lectronic **K**ey **M**anagement **S**ystem
(U//FOUO) EM01	The module number for the 802.3 Ethernet module that attaches to the SecNet 54® cryptographic module (i.e., KIV-54).
(U//FOUO) EMOD	**E**thernet **Mod**ule
(U) ESP	**E**ncapsulated **S**ecurity **P**ayload
(U) EULA	**E**nd **U**ser **L**icense **A**greement
(U) EXT	**Ext**ernal

-F-

(U//FOUO) Factory Default Condition	A KIV-54 that meets the following criteria: a single default entry in the ACL, no keys loaded, and no tunnels defined.
(U) FAQ	**F**requently **A**sked **Q**uestions
(U) FCC	**F**ederal **C**ommunications **C**ommission
(U//FOUO) FF	**F**IRE**F**LY. A technique to electronically negotiate (using a protocol exchange) traffic encryption keys using pre-placed key generation material, called vectors, between two independent nodes without human intervention.
(U) FPGA	**F**ield **P**rogrammable **G**ate **A**rray
(U) FW	**F**irmware

-G-

(U) GHz	**G**igahertz (10^9)
(U) GMT	**G**reenwich **M**ean **T**ime

-H-

(U//FOUO) HAIPE®	**H**igh **A**ssurance **I**nternet **P**rotocol **E**ncryptor

(U) HAIPIS	**H**igh **A**ssurance **I**nternet **P**rotocol **I**nteroperability **S**pecification
(U) Hex	**H**exidecimal. A base-16 number system that consists of 16 unique symbols, 0 to 9 and A to F.
(U//FOUO) HNP	**H**ost **N**etwork **P**rocessor
(U) HTML	**H**yperText **M**arkup **L**anguage. A language designed for the creation of Web pages and other information viewable in a browser.
(U) HTTPS	**H**ypertext **T**ransfer **P**rotocol **S**ecure. An extension of the HyperText Transfer Protocol (HTTP) protocol that supports sending data securely over the Web.
(U) Hz	**H**ertz
(U) HW	**H**ardware

-I-

(U) ICMP	**I**nternet **C**ontrol **M**essage **P**rotocol
(U) IEEE	**I**nstitute of **E**lectrical and **E**lectronics **E**ngineers
(U) IGMP	**I**nternet **G**roup **M**anagement **P**rotocol. A communications protocol used to manage the membership of IP multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships.
(U//FOUO) IKE	**I**nternet **K**ey **E**xchange. A protocol used to generate a common key between two HAIPE® devices by using public key techniques.
(U//FOUO) INE	**I**nline **N**etwork **E**ncryptor. The networking device that is inserted into a network path that encrypts and decrypts packets traversing the path.
(U) Infrastructure	A wireless communications network that combines Access Points, mobile nodes and fixed nodes. All communication occurs through the Access Point. Individual stations cannot communicate directly with each other.
(U) Interoperable	An interoperable device works together to communicate data through a network path.
(U) IP	**I**nternet **P**rotocol
(U) IP Address	A unique number assigned to a node to designate it on a TCP/IP network.
(U) IPSEC	**I**nternet **P**rotocol **S**ecurity
(U) ISM	**I**ndustrial, **S**cientific, and **M**edical Band

(U//FOUO) ISAKMP	**I**nternet **S**ecurity **A**ssociation and **K**ey **M**anagement **P**rotocol

-J-

(U) J2SE	**J**ava **2** **S**tandard **E**dition
(U) JRE	**J**ava **R**untime **E**nvironment

-K-

(U//FOUO) KIV-54	The module number of the SecNet 54® cryptographic module.
(U//FOUO) KMID	**K**ey **M**anagement **I**dentification. A 10-digit decimal number of the unique key ID assigned by EKMS Central Facility (CF).

-L-

(U) LAN	**L**ocal **A**rea **N**etwork
(U) LC	**L**ampert **C**onnector
(U) LED	**L**ight-**E**mitting **D**iode

-M-

(U) MAC	**M**edium **A**ccess **C**ontrol
(U) Mbps	**M**ega**b**its **p**er **s**econd (10^6)
(U) MD	**M**essage **D**igest **A**lgorithm
(U) MDI/MDIX	**M**edium **D**ependent **I**nterface/**M**edium **D**ependent **I**nterface Crossover
(U) MIC	**M**essage **I**ntegrity **C**heck
(U) MODP	**M**ore **M**odular **E**xponential
(U//FOUO) MTEK	**M**ain **T**raffic **E**ncryption **K**ey

-N-

(U) NSA	**N**ational **S**ecurity **A**gency

-O-

(U) OFDM	**O**rthogonal **F**requency **D**ivision **M**ultiplexing

-P-

(U) PCMCIA	**P**ersonal **C**omputer **M**emory **C**ard **I**nternational **A**ssociation
(U) PEM	**P**rivacy **E**nhanced **M**ail
(U) PMTU	**P**ath **M**aximum **T**ransfer **U**nit
(U) PoE	**P**ower **o**ver **E**thernet. A solution where electrical current is run to networking hardware over the Ethernet Category 5 or higher data cabling.
(U//FOUO) PPK	**P**re-**P**laced **K**ey
(U) PSEQN	**P**acket **S**equence **N**umber
(U) PT	**P**lain **T**ext. Textual data in American Standard Code for Information Interchange (ASCII) format. Messages that are not encrypted.

-R-

(U) Red Network	A classified (or secure) network.
(U) RF	**R**adio **F**requency
(U) RMA	**R**eturn **M**aterial **A**uthorization
(U//FOUO) RM01	The model number for the 802.11 wireless radio that attaches to the SecNet 54® cryptographic module (i.e., KIV-54).
(U//FOUO) RMOD	**R**adio **Mod**ule
(U) RX	**R**eceive or **R**eceiver

-S-

(U//FOUO) SA	**S**ecurity **A**ssociation. A set of policy and key(s) used to protect information.
(U//FOUO) SAD	**S**ecurity **A**ssociation **D**atabase
(U) SHA	**S**ecure **H**ash **A**lgorithm

(U) SMA	**S**ub**M**iniature Version **A**
(U//FOUO) SN	**S**ec**N**et
(U) SP	**S**ecurity **P**olicy
(U//FOUO) SPD	**S**ecurity **P**olicy **D**atabase
(U) SPI	**S**ecurity **P**arameter **I**ndex
(U) SSID	**S**ervice **S**et **Id**entifier. The name of a WLAN. All wireless devices on a WLAN employs the same SSID to communicate with each other. The SSID is a sequence of alphanumeric characters that are case sensitive and have a 32-character maximum length.
(U) SSL	**S**ecure **S**ocket **L**ayer. A protocol for encryption and authentication of Internet connections.
(U) SSL Certificates	Certificates that ensure two-way authentication with both a server side certificate and a client side certificate.
(U) STA	**Sta**tion
(U//FOUO) Static HAIPE® IKE Tunnel	A tunnel that uses NSA Type-1 FIREFLY Vectors, where the HAIPE® device at each end of the tunnel has the same vectors loaded and associated with the static tunnel. This type of tunnel must be configured and manually established prior to use. Static HAIPE® IKE tunnels establish a MTEK through a negotiation process with another HAIPE®. The MTEK negotiation is initiated from the HMI after configuration.
(U//FOUO) Static PPK Tunnel	A tunnel that uses NSA Type-1 PPKs, where the HAIPE® device at each end of the tunnel has the same HAIPE® PPK(s) loaded and associated with the static tunnel. This type of tunnel must be manually configured prior to use and is assumed to be established once properly configured. Configuration consists of assigning PPKs to chains, assigning the chains to a set of IP addresses that represent HAIPE® devices on each end of the tunnel, and then assigning the tunnel to a security policy.

-T-

(U) TCP	**T**ransmission **C**ontrol **P**rotocol
(U) TKIP	**T**emporal **K**ey **I**ntegrity **P**rotocol
(U) TLS	**T**ransport **L**ayer **S**ecurity
(U) TOS	**T**ype **o**f **S**ervice

(U) TTL	**T**ime **t**o **L**ive
(U) TX	**T**ransmit or **T**ransmitter
(U) Tunnel	The pathway carrying Type-1 encrypted information over a Black network from one HAIPE® compliant device (e.g., a SecNet 54® device) to another HAIPE® compliant device. All HAIPE® tunnel types require that the destination device has the same security level as the originating device to establish a tunnel.

-U-

(U) UNII	**U**nlicensed **N**ational **I**nformation **I**nfrastructure
(U) UPS	**U**ninteruptable **P**ower **S**ource
(U) URL	**U**niform **R**esource **L**ocator. The global address of documents and other resources on the Web. The first part of the address indicates what protocol to use, and the second part specifies the IP address or domain name where the resource is located.

-V-

(U) VAC	**V**olts of **A**lternating **C**urrent
(U) VPN	**V**irtual **P**rivate **N**etwork. A private data network that uses a tunneling protocol and security procedures.

-W-

(U) WAN	**W**ide **A**rea **N**etwork. A long-distance communications network that covers a wide geographical area such as a state or country.
(U) WB	**W**ireless **B**ridge. Connectivity between a wireless LAN and wired networks, or additional wireless LANs, as applicable.
(U) WEB Browser	A software application that enables a user to display and interact with text, images, music, games and other information and is typically located on a Web page at a Web site on the World Wide Web (WWW) or LAN. Web browsers may also access data by Web servers in private networks or content in file systems.
(U) WEP	**W**ired **E**quivalent **P**rivacy
(U) WLAN	**W**ireless **L**ocal **A**rea **N**etwork

(U) WPA-PSK	**W**i-Fi **P**rotected **A**ccess-**P**re-**S**hared **K**ey

-X-

(U) XMOD	**E**xternal **Mod**ule

-Z-

(U//FOUO) Zeroize	The removal of the ACL, keys, and tunnels from the KIV-54 by selecting the **ZEROIZE** button on a SecNet 54® configuration Web page; or the removal of the ACL, keys, vectors, tunnels, PPK Chains, and network settings (i.e., a factory reset configuration) from the KIV-54 by pressing the Panic Zeroize buttons with power on or off.

Appendix B

(U) FREQUENTLY ASKED QUESTIONS (FAQ)S

B.1 (U) INTRODUCTION

(U) This section is designed to help the User maintain the equipment for maximum efficiency and security. Included are answers to the most commonly asked questions, which will help clarify an understanding of the cryptographic and external modules' functionality. Users should contact the Administrator for additional assistance regarding administrative functions (e.g., adding new Users, loading keys, or configuring tunnels).

(U) If the information presented in this User manual does not solve the problem and technical support is required, contact the Technical Support group as indicated in **APPENDIX C, TECHNICAL SUPPORT AND CONTACT INFORMATION**.

(U) The following information must be provided when contacting technical support:

- (U) The type of configuration that is being connected.
- (U) The model number of the external module.
- (U) The Electronic Serial Number of the KIV-54.
- (U) The software (firmware (FW)) version of the KIV-54 and external modules.
- (U) The HW version of the KIV-54.

U) Note that the information for the last four items listed above is located on the configuration Web page **Maintenance** menu **About** tab.

B.2 (U) SECNET PRODUCT FAMILY

Q: (U//FOUO) **What is the difference between the SecNet 54® and SecNet 11 Plus?**
A: (U//FOUO) Both the KIV-54RM01 and the SecNet 11 Plus products offer users secure wireless local area networking solutions, and the SecNet 54® Ethernet product (KIV-54EM01) offers users In-line Network Encryption (INE) networking solutions.

(U//FOUO) SecNet 54® wireless product (KIV-54RM01) and the SecNet 54® Ethernet product (KIV-54EM01) are NOT replacements for SecNet 11; both are additions to Harris' overall product offerings. Each product provides different capabilities as follows:

(U//FOUO) **SecNet 11 Plus is ideal for missions and/or environments requiring:**

- (U//FOUO) Secret Level Data (COMSEC)
- (U) 802.11b Wireless Communication
- (U//FOUO) Encryption of all Ethernet/IP Addresses & 802.11 MAC packets (Link Encryption)
- (U) Low Cost
- (U) Low Power Usage
- (U) Small Size
- (U) Ultra Lightweight
- (U) PCMCIA Form Factor

- (U//FOUO) Crypto Embedment
- (U//FOUO) Simple Key Management

(U) KIV-54RM01 is ideal for missions and/or environments requiring:

- (U//FOUO) Up to Top Secret/SCI Level Data (COMSEC)
- (U) 802.11 a, b, g Wireless Communication
- (U//FOUO) HAIPIS 1.3.5 Compatibility (IPSec)
- (U) Interoperable with Commercial Networks
- (U) Both Copper and Fiber-Based Ethernet Networks/Users
- (U) PoE Compatible
- (U) Ruggedized Enclosure
- (U) Single device can operate as an Ad Hoc client or infrastructure Wireless Bridge (WB)/Access Point (AP)
- (U//FOUO) Modular concept allows use of KIV-54 cryptographic module with additional future transmission media modules.

(U) KIV-54EM01 is ideal for missions and/or environments requiring:

- (U//FOUO) Up to Top Secret/SCI Level Data (COMSEC)
- (U//FOUO) HAIPIS 1.3.5 Compatibility (IPSec)
- (U) Interoperable with Commercial Networks
- (U) Both Copper and Fiber-Based Ethernet Network/Users
- (U) Dual 100Base-TX/10Base-T side electrical interfaces
- (U) POE Compatible
- (U) Ruggedized Enclosure
- (U//FOUO) Modular concept allows use of KIV-54 cryptographic module

Q: (U) Is SecNet 54® a replacement for SecNet 11 Plus?

A: (U//FOUO) The SecNet 54® wireless product (KIV-54RM01) is NOT a replacement for SecNet 11; it is an addition to Harris' overall product offerings. Refer to the response above for additional information.

Q: (U) Is KIV-54 HAIPIS Compliant?

A: (U//FOUO) The KIV-54 cryptographic module is Full HAIPIS 1.3.5 compliance, supporting multiple, PPK segments and editions, allowing for up to a year of operational crypto key material. Using the Accordian 1.3 key update/changeover in accordance with the HAIPIS 1.3.5, KIV-54 is interoperable with other COMSEC HAIPIS 1.3.5 key compliant devices. The KIV-54 also supports FIREFLY and Enhanced FIREFLY exchange.

Q: (U) What are "advanced key management features"?

A: (U//FOUO) The KIV-54 cryptographic module is Full HAIPIS 1.3.5 compliance, supporting multiple, PPK segments and editions, allowing for up to a year of operational crypto key material. Using the Accordian

1.3 key update/changeover in accordance with the HAIPIS 1.3.5, KIV-54 is interoperable with other COMSEC HAIPIS 1.3.5 key compliant devices. The KIV-54 also supports FIREFLY and Enhanced FIREFLY exchange.

Q: (U) What are the peak wireless throughput expectations?

A: (U//FOUO) The RM01 wireless radio module supports datalink rates up to 54 Mbps. Throughput is a function of application and packet structure.

Q: (U) How is multicast handled?

A: (U//FOUO) KIV-54RM01 handles multicast packets in accordance with industry standards using PPK in accordance with HAPIS 1.3.5.

Q: (U) Is 802.11e - QoS supported?

A: (U//FOUO) KVI-54RM01 does not support 802.11e Quality of Service (QoS).

Q: (U) Why can't I enable the radio?

A: (U//FOUO) The radio cannot be enabled by a User unless TBD. Only an Administrator can enable the radio of an Access Point or Wireless Bridge.

Q: (U) When the radio is in the WB or Ad Hoc Station mode, why is it not operating on the channel selected during RM01 configuration?

A: (U//FOUO) When in WB or Ad Hoc mode, the radio first scans all channels searching for another radio that is operating in a similar mode and within range. If it finds one that has the same SSID, it will associate with that radio on whatever channel that radio is operating.

Q: (U) After installation of the Harris Corporation GCSD SecNet 54® SSL Certificate, why does the Security Alert window, displayed during the login process, contain the following message?

The name on the security certificate is invalid or does not match the name of the site.

A: (U) This is an expected warning due to the lack of support by Internet Explorer (version 6.0) in recognizing wildcards as valid characters for security certificate names. Internet Explorer does not recognize the SecNet 54® IP address as the address provided by the server.

Appendix C

(U) TECHNICAL SUPPORT AND CONTACT INFORMATION

(U) SecNet 54® Product Family Support Policy

(U) Harris Corporation, RF Communications Division (RFCD) provides free help desk support throughout the warranty period of the SecNet 54® purchased products. Technical support is available 24 hours a day, seven days a week via the help desk support center at 1-585-244-5830, 1-585-242-4319, 1-800-264-8080 (USA toll-free) or e-mail at rfcsrvc@harris.com. Frequently Asked Questions (FAQs), technology support, software updates, advisories, order support, and general information can be accessed via the SecNet 54® product family Website at **http://www.secnet54.harris.com.**

(U) Additional services may be procured if the support required goes beyond routine technical assistance. SecNet 54® services are available for tasks including consultations, site surveys, and installations. Classroom training is available at the Harris RFCD campuses in Melbourne, Florida or Rochester, New York. Additionally, classroom training can be arranged to be held on-site at a customer facility. System user manuals and quick reference guides are available via the website noted above.

(U) Technical Support applies to model numbers:

- (U) KIV-54RM01
- (U) KIV-54EM01
- (U) KIV-54
- (U) RM01
- (U) EM01
- (U) SN54-FC01

Appendix D

(U) WARRANTY

(U) SecNet 54® Product Family Warranty

(U) Seller warrants the items ordered hereunder at the time of final acceptance to be free from defects in material and workmanship. Seller's liability under this Warranty shall commence on the date of shipment and terminate 12 months thereafter. Written notice of any defects shall be given to Seller upon discovery and Seller shall promptly correct such defects by repair or replacement, at its option, without charge, either FOB Seller's plant or service in the field. Seller uses new and reconditioned parts to satisfy warranty repairs and replacements under the terms of this warranty. Defective articles shall not be returned to the Seller's factory without the prior written authorization of the Seller. Call 1-585-244-5830 to obtain a Return Material Authorization (RMA) number. Seller shall have the right of final determination as to the existence and cause of any claimed defect. In no event shall Seller's liability under this Warranty exceed the cost of repair or replacing such defective item and under no circumstances shall Seller be liable for special or consequential damages.

(U) Specifically excluded from the terms of this Warranty are:

1. (U) This provision does not apply to any defects which occur as a result of:

   a. (U) Acts of God.

   b. (U) Physical impact, crash or foreign object damage.

   c. (U) Improper maintenance, storage, modification or alteration by the Buyer or Buyer's Customer.

   d. (U) The Buyer's or Buyer's Customer operation of the items delivered under this contract with any accessory, equipment or part not specifically approved by the Seller unless the Buyer furnishes clear and convincing evidence that such accessory, equipment, or part was not a cause of the defect.

   e. (U) Normal wear and tear. The parties recognize that certain parts have a limited service life and will wear out through normal use.

   f. (U) Products subjected to misuse, detrimental exposure, or involved in an accident.

   g. (U) Products subject to any kind of negligence by a part other than Seller.

   h. (U) Defects caused by improper storage, use, installation, or maintenance.

2. (U) Seller is not responsible under this provision for defects with respect to items not provided by Seller or its subcontractors.

3. (U) The provisions of this clause do not cover liability for loss, damage, or injury to third parties.

4. (U) In the event the cause of returned product is determined to be consistent with any of the items in numbers 1 through 3 above, Buyer may be subject to an evaluation and repair charge.

5. (U) ALL IMPLIED WARRANTIES OR MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE EXCLUDED FROM ANY OBLIGATION UNDER THIS CONTRACT. IN NO EVENT SHALL THE CONTRACTOR BE LIABLE FOR ANY CONSEQUENTIAL, INCIDENTAL, SPECIAL, PUNITIVE OR OTHER DAMAGE AS A RESULT OF DEFICIENCIES IN SUPPLIES OR SERVICES DELIVERED UNDER THIS CONTRACT.

6. (U) To repair any SecNet 54® product (Cryptographic Module, External Module, or Key Fill Cable) after the 12 month warranty has expired, call 1-585-244-5830 to obtain a Return Material Authorization (RMA) number and an estimated cost for repair.

(U) SecNet 54® Product Family Return Policy

(U) Within 30 days of shipment of the order, Buyer may return all unused items ordered for a full refund minus a 20% re-stocking charge for all items. Shipping & handling charges are non-refundable. Buyer must include all original packing materials, manuals and accessories with the product to avoid any additional fees. Product should not be returned to the Seller's factory without the prior written authorization of the Seller. Call 1-585-244-5830 to obtain a RMA number. Restocking charging and credits for returns will be processed upon Seller’s satisfactory completion of inspection and test.

This Page Intentionally Left Blank

Appendix E

(U) SPECIFICATIONS

E.1 (U) RM01 SPECIFICATIONS

(U//FOUO) The RM01 is based on a standard 802.11a/b/g chip set and supports data rates up to 54 Mbps. It is compatible with Commercial Off-the-Shelf (COTS) WLAN equipment. The RM01 operates in the 2.4 GHz license free Industrial, Scientific and Medical band and the 5 GHz Unlicensed National Information Infrastructure (UNII) band. The US band for 802.11a is split into three operating bands and allows power as indicated below. Data is transmitted over a half duplex radio channel that operates up to 11 Mbps in 802.11b mode and up to 54 Mbps in 802.11a/g modes. The RM01 can be configured as an Access Point, Wireless Bridge, Infrastructure Client, or Ad Hoc Station.

(U) IEEE 802.11 a/b/g Standard Compatible Specifications

(U) Data Rates:

- (U//FOUO) 802.11a: 6, 9, 12, 18, 24, 36, 48, 54 Mbps
- (U//FOUO) 802.11b: 1, 2, 5.5,11 Mbps
- (U//FOUO) 802.11g: 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps

(U) Frequency Bands:

- (U//FOUO) ISM 2.412 to 2.462 GHz (802.11b/g modes)
- (U//FOUO) U-NII lower 5.15 to 5.25 GHz; U-NII middle 5.25 to 5.35 GHz; U-NII upper 5.725 to 5.85 GHz (802.11a mode)

(U) Channels:

- (U//FOUO) 802.11b/g: 3 non-overlapping (Selections: 1 through 11)
- (U//FOUO) 802.11a: 12 non-overlapping (Selections: 36, 40, 44, 48, 52, 56, 60, 64,149,153, 157, and 161)

(U) Configurable Radio MAC Modes:

- (U//FOUO) Access Point
- (U//FOUO) Wireless Bridge
- (U//FOUO) Infrastructure Station
- (U//FOUO) Ad Hoc Station

(U) Transmit Power at SMA Ports:

- (U//FOUO) 14 dBm Typical @ 54 Mb
- (U//FOUO) 17 dBm Typical @ 11 Mb

(U) Antenna (included):

- (U//FOUO) Dual Diversity Swivel dipoles
- (U//FOUO) 0 dBi Nominal @ 2.4 GHz
- (U//FOUO) 0 dBi Nominal @ 5 GHz

(U) Transmit Power Settings:

- (U//FOUO) Full, 1/2, 1/4, 1/8 (Minimum)

(U) Rx Sensitivity:

UNCLASSIFIED//FOUO

dBm	Mbps	GHz
-94	1	2.4
-88	11	2.4
-88	6	5
-82	24	5
-75	54	2.4
-73	54	5

UNCLASSIFED//FOUO

(U) Range: (Clear Line of Site)

- (U//FOUO) 54 Mb: 800 feet outdoor, 300 feet indoor @ 10% per Range
- (U//FOUO) 11 Mb: 1800 feet outdoor @ 8% per Range
- (U//FOUO) 1 Mb: 2900 feet outdoor @ 8% per Range

(U) Note: Actual values will vary with conditions.

E.2 (U) KIV-54RM01 PARAMETERS AND SPECIFICATIONS

(U) Operating Temperature:

- (U//FOUO) -10 C to +40 C

(U) Storage Temperature:

- (U//FOUO) -25 C to +70 C

(U) Power Dissipation:

- (U//FOUO) 8W @ 25 C

(U) Size:

- (U//FOUO) 3.18 in. x 5.26 in. x 1.13 in.

(U) Weight:

- (U//FOUO) 11 oz. (with antennas)

(U) Power Supplies:

- (U//FOUO) Auto sensing dual DC power inputs for AC adapter and battery
- (U//FOUO) External AC adapter included: 120 - 220 Vac, 50-60 Hz
- (U//FOUO) External Battery input: 14 to 30 Vdc

- (U//FOUO) 802.3af POE through RJ45 connector
- (U//FOUO) Smart power selection senses power adapter, POE, and battery

(U) Data Interfaces (Red Side):

- (U//FOUO) 10/100 base-T wired 802.3 Ethernet
- (U//FOUO) 100 base-FX optical 802.3 Ethernet

(U) Key Management:

- (U//FOUO) Red key fill via DS-101 interface
- (U//FOUO) Over-the-Air/Over-the-Network zeroization
- (U//FOUO) Mechanical "Panic" zeroization

(U) Certification:

- (U//FOUO) Controlled Cryptographic Item (CCI)
- (U//FOUO) NSA-certification of Top Secret (TS) and below

(U) Encryption:

- (U//FOUO) The SecNet 54® device can inter-operate with a HAIPIS 1.3.5 compliant Inline Network Encryptor (INE) using pre-placed symmetric keys if both devices have been properly manually configured.

(U) Configuration:

- (U//FOUO) Secure Web-based access from host
- (U//FOUO) Remote configuration over Red network
- (U//FOUO) Web-based IPSec configuration

(U) Indicators:

- (U//FOUO) Clear indication of mode and status via LEDs: 4 on KIV-54 and 6 on RM01

Appendix F

(U) KIV-54RM01 FACTORY DEFAULT SETTINGS

F.1 (U) INTRODUCTION

(U//FOUO) This appendix contains the factory default values for the KIV-54 and the RM01 configuration items. When the KIV-54 and the RM01 modules arrive from the factory, they will contain these preset values.

F.2 (U) KIV-54 FACTORY DEFAULT VALUES

(U//FOUO) The KIV-54 can be reset to the factory default values by pressing the Panic Zeroize buttons with power on. Refer to Section 2-3.1.2.2 for additional information about resetting the KIV-54 back to the factory default values.

(U//FOUO) The following table lists the KIV-54 configuration items and the factory default value.

UNCLASSIFIED//FOUO

Configuration Item	Value
HAIPE® Network	
• Device Host Name	default
• Red Network	
MAC Address	Unique to each KIV-54; not changed by factory reset.
IP Address	192.168.1.54
Subnet Mask	255.255.0.0
Gateway	192.168.1.54
• Black Network	
IP Address Type	Static Entry
IP Address	10.10.10.54
Subnet Mask	255.255.0.0
Gateway	10.10.10.54
Security	
• Classification Level	Inhibit
• Default Traffic Flow Security (TFS)	
Crypto Block Size	48
Fixed Packet Size	Enabled
Fixed Packet Size	800
Path MTU	N/A

Configuration Item	Value
Time to Live (TTL)	255
PSEQN Window Size	64
Do Not Fragment Policy	Clear Bit in Black IP Header
Type of Service (TOS)/ DiffServ Policy	Clear Field in Black IP Header
TOS/DiffServ Value	N/A
• Global Device TFS Settings	
Path MTU Discovery	Disabled
IGMP	Enabled
Black Side Reply to Ping	Enabled
• Key(s)	
Pre-Placed Keys (PPKs)	None
PPK Chains	None
FIREFLY Vectors	None
Basic and Alternate P^3 dePAC Moduli	None
• Tunnels	
Tunnels (PPK and HAIPE® IKE)	None
SPD Tables	None
Dynamic Discovery - Community of Interest (COI) Table	None
Routes	
• Routing Information Protocol version 2 (RIPv2)	
Process Incoming RIP Messages	Disabled
Send Default Route Attachments	Disable
SA Reachability Advertisements	Disabled
Outgoing Default Route Metric	1
Authentication	None
Authentication Password	N/A
Red-side Routing Table	None

Configuration Item	Value
Access Control List	All User accounts are removed by factory reset.
Date and Time	Current real time clock time setting not changed by factory reset.

UNCLASSIFIED//FOUO

F.3 (U) RM01 FACTORY DEFAULT VALUES

(U//FOUO) The RM01 values are reset with the factory reset function. The default values are reset with the **Default Settings** button on the **RM01** page in the configuration Web pages. Refer to Section 3.2.6 for additional information on resetting the default values. The following table lists the factory default values for the RM01.

UNCLASSIFIED//FOUO .

Configuration Item	Value
RM01	
• SSID	secnet54_default_SSID
• Operational Mode	Infrastructure Mode Station
• RF Band	802.11 b/g
• Operating Channel	6
• TX Data Rate	Best
• TX Power Level	Full
• Antenna	Best
VPN Security	
• General	
VPN Configuration	Disabled
VPN Status	Disconnected
Phase 1 Key Management	IKE
Aggressive Mode	Enabled
Local IP Configuration	Static Entry
Local IP Address	10.10.10.54
Local Subnet Mask	255.255.0.0
Local Gateway	10.10.10.54

Configuration Item	Value
Remote Gateway	192.168.0.1
Remote Subnet	127.0.0.1
Remote Netmask	255.255.0.0
• Authentication	
Authentication Method	Preshared Key
• Phase 1	
Diffe-Hellman (DH) Group	DH Group 2 (MODP1024)
Encryption Type	AES-128
Digital Signature	MD5 Auth
Lifetime (seconds)	1400
• Phase 2	
Prefect Forward Secrecy (PFS)	Enabled
Diffe-Hellman (DH) Group	DH Group 2 (MODP1024)
Authentication Type	AES-128
Digital Signature	MD5 Auth
Lifetime (seconds)	3600

UNCLASSIFIED//FOUO

This Page Intentionally Left Blank

(U) IMPORTING SECNET 54® SSL CERTIFICATES INTO WEB BROWSERS

G.1 (U) INTRODUCTION

(U) This Appendix describes importing the SecNet 54® SSL Certificates from the local computer's desktop into the following Web browsers:

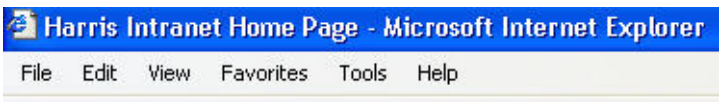
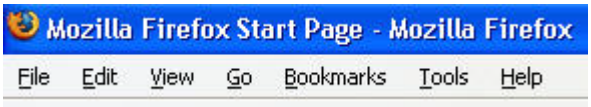
- (U) Internet Explorer (IE) (version 6.0)
- (U) Mozilla Firefox (versions 1.0.x and 1.5.x)
- (U) Netscape (version 7.2)

(U//FOUO) Before the SecNet 54® Web-based configuration pages can be used, the two SecNet 54® SSL Certificates must be installed into the Web browser. This installation must be completed for each individual computer and browser that are to be used for SecNet 54® configuration. Depending on the operating system, the process may need to be repeated for each user of a given computer.

(U//FOUO) The two certificates are the Client Certificate and the Certification Authority (CA) Certificate. Unlike most Web sites, the SecNet 54® requires a Client Certificate. It will refuse connection with any browser that does not contain the correct Client Certificate. Likewise, the browser will not trust the certificate presented by the SecNet 54® unless it has a CA Certificate for the signing authority of the SecNet 54® host certificate. The method of installing the certificates will vary by browser and operating system. This appendix contains examples of certificate installation instructions for common Web browsers that may be applicable.

(U//FOUO) Additional information about the SecNet 54® SSL Certificates are described in Section 3.2.1 of this manual. The certificate import process begins at each Web browser's main menu bar. Three common menu bars are illustrated in the following table.

UNCLASSIFIED

Browser	Main Menu Bar
Microsoft Internet Explorer	
Mozilla Firefox	
Netscape	

UNCLASSIFIED

Appendix G (U) Importing SecNet 54 SSL Certificates into Web Browsers

NOTE

(U//FOUO) To ensure that the SecNet 54® Web pages are displayed in a specific Web browser on a local computer (i.e., when Web pages are accessed from the SMU program), the specific Web browser must be set as the operating system default browser for that computer. Refer to the browser's online **Help** for information on setting the browser as the default.

G.2 (U) IMPORTING THE SECNET 54 SSL CERTIFICATES USING THE IE WEB BROWSER

(U//FOUO) The SecNet 54 SSL CA Certificate must be installed before the SecNet 54 SSL Client Certificate. When the SSL CA Certificate is installed first, the browser will trust the SSL Client Certificate. If the SSL Client Certificate is not installed, the SecNet 54® device will not allow the connection to the Web browser.

NOTE

(U) The following certificates and associated data are examples. The actual certificate dates and associated data may differ when certificates are revised.

(U//FOUO) In addition to installing SecNet 54 SSL CA and SSL Client Certificates from the IE Web browser's main menu (version 6.0 and higher), the installation process can also begin from the certificates location. This installation process is described in Section G.2.3.

G.2.1 (U) Importing the SecNet 54 SSL CA Certificate Using the IE Web Browser (Version 6.0)

(U//FOUO) The SecNet 54 SSL CA Certificate import process begins at the IE Web browser's (version 6.0) main menu bar (refer to Section G.1). Selecting **Internet Options** from the **Tools** submenu displays the **Internet Options** window. Selecting the **Content** tab from the **Internet Option** window displays three areas, including the Certificates area.

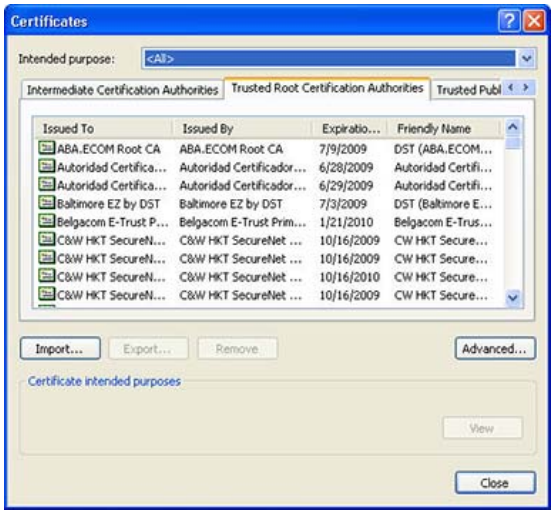
UNCLASSIFIED

UNCLASSIFIED

(U) The **Certificates...** button selection displays the **Certificates** window, and selecting the **Trusted Root Certifications Authorities** tab displays a listing of the current certificates installed on the local computer. The **Import...** button selection launches the **Certificate Import Wizard**.

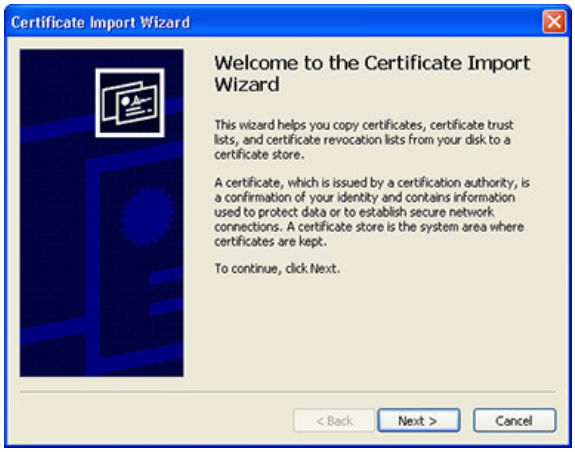
Appendix G (U) Importing SecNet 54 SSL Certificates into Web Browsers

UNCLASSIFIED



UNCLASSIFIED

UNCLASSIFIED



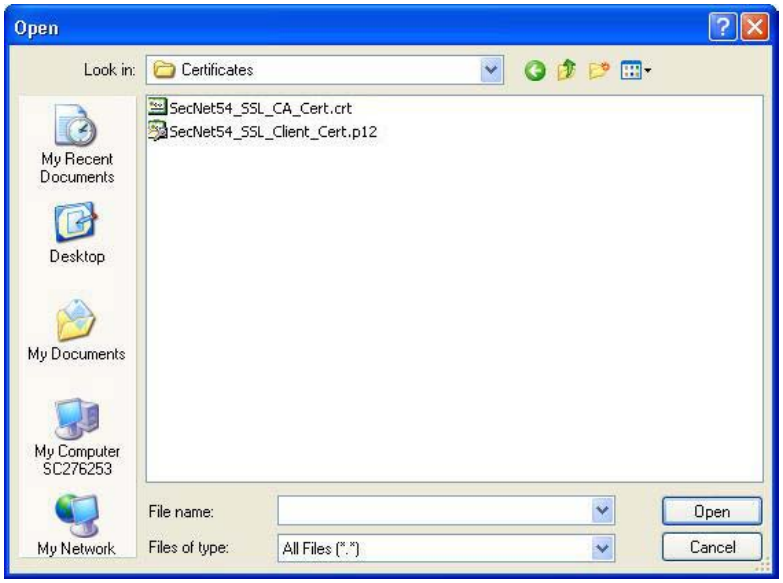
UNCLASSIFIED

(U//FOUO) The **Next >** button selection displays the **File to Import** page in the wizard. Selecting the **Browse...** button allows the User to locate the SecNet 54 SSL CA Certificate in the **Open** window.

UNCLASSIFED

UNCLASSIFIED

UNCLASSIFIED//FOUO

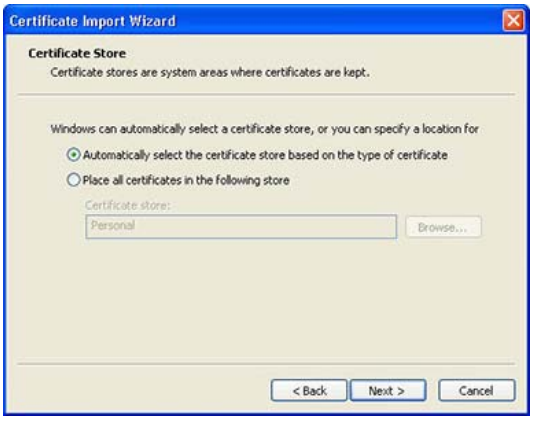


UNCLASSIFEID//FOUO

Appendix G (U) Importing SecNet 54 SSL Certificates into Web Browsers

(U//FOUO) The “Look in” drop-down list box selection displays the drive containing the certificate. The selection of “All Files (*.*)” from the drop-down list box in the “Files of type” displays all file types. Double-clicking the SecNet_54_SSL_CA_Cert.crt file displays the file path in the “File name” of the **Certificate Import Wizard** window. The wizard’s **Next >** button selection displays **Certificate Store** page.

UNCLASSIFIED



UNCLASSIFIED

(U) Selecting the radio button for “Automatically select the certificate store based on the type of certificate” specifies the criteria for the certificate store location. And, the **Next >** button selection displays a certificate import complete message within the wizard.

(U//FOUO) The **Finish** button selection completes the import and displays a **Security Warning** window from which to verify the SecNet 54 Root CA Certificate.

UNCLASSIFIED//FOUO

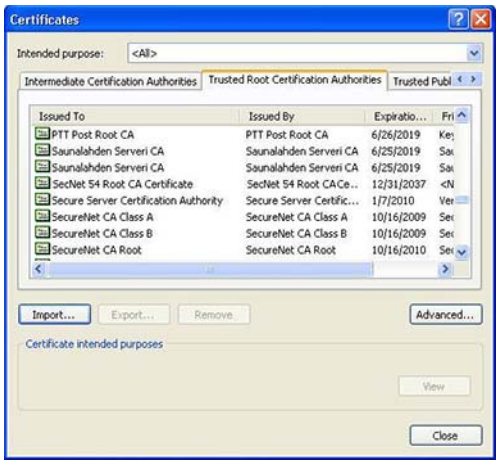
UNCLASSIFIED//FOUO

(U) The **Yes** button selection displays the following message in the wizard:

The import was successful.

(U//FOUO) The **OK** button selection removes the wizard window and redisplays the **Certificates** window. The **Trusted Root Certification Authorities** tab displays the SecNet54 Root CA Certificate listed in the "Issued To" and "Issued By" columns.

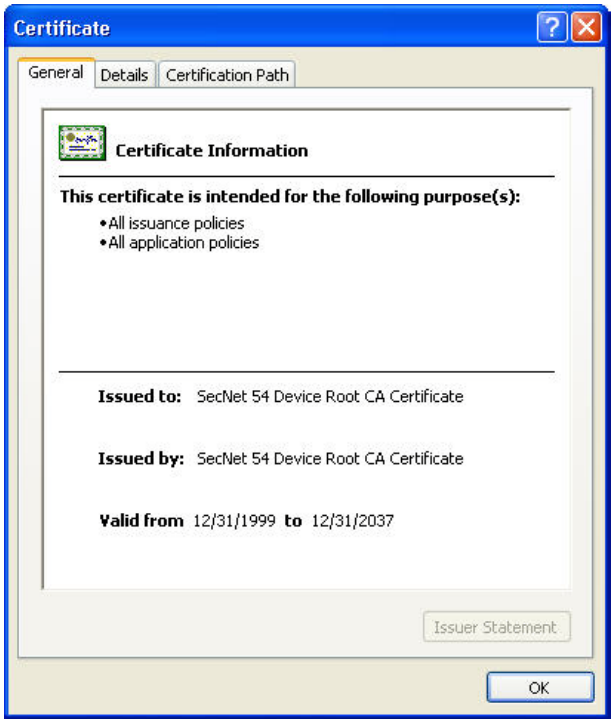
UNCLASSIFIED//FOUO



UNCLASSIFIED//FOUO

(U//FOUO) Selecting the CA Certificate activates the **View** button. The **View** button selection displays the SecNet 54 Root CA Certificate, indicating the certificate's intended purpose(s).

UNCLASSIFIED//FOUO



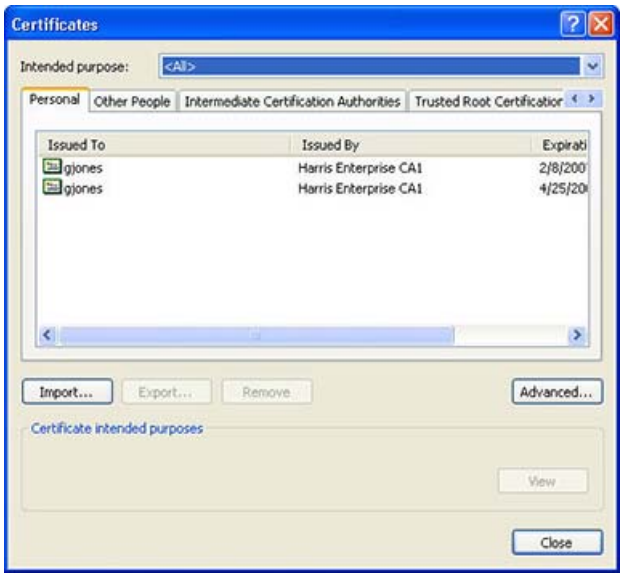
UNCLASSIFIED//FOUO

(U) The **OK** button selection closes the **Certificate** window, redisplaying the **Trusted Root Certification Authorities** tab in the **Certificates** window.

(U//FOUO) The client side certificate is also imported from the **Certificates** window as described in the following section, G.2.2. The SecNet 54 SSL Client Certificate must be installed to complete the two-way authentication.

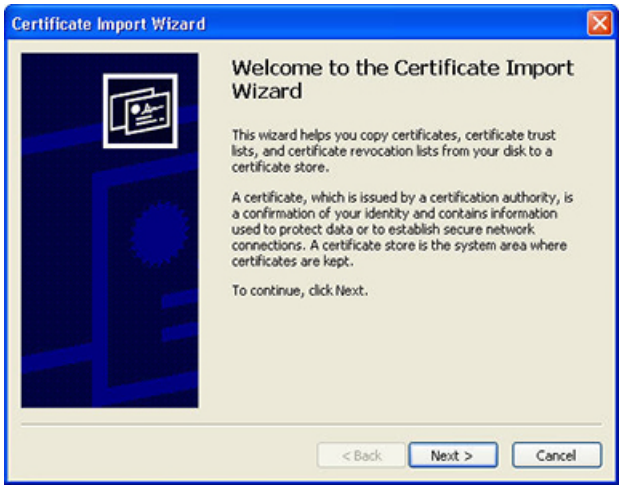
G.2.2 (U) Importing the SecNet 54 SSL Client Certificate Using the IE Web Browser (Version 6.0)

(U) Once the SSL CA Certificate has been imported, the SSL Client Certificate can be installed. Selecting the left vertical arrow in the upper right hand corner of the **Certificates** window and scrolling to the left display the **Personal** tab. When selected, the **Personal** tab page displays a listing of the current personal certificates that have been issued.



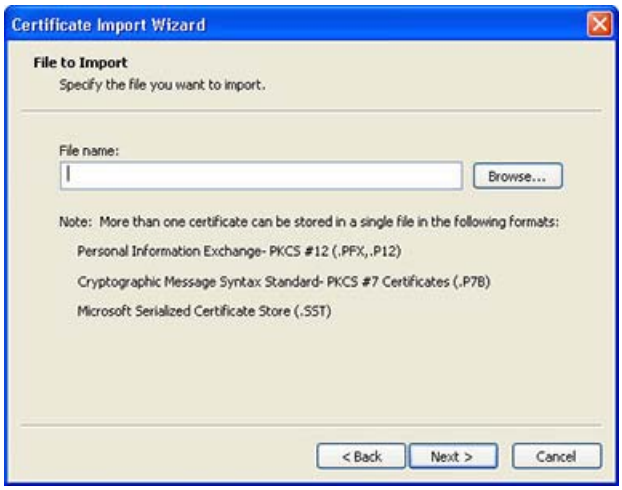
(U) The **Import...** button selection launches the **Certificate Import Wizard**, and the wizard's **Next >** button selection displays the **File to Import** page in the wizard.

UNCLASSIFIED



UNCLASSIFIED

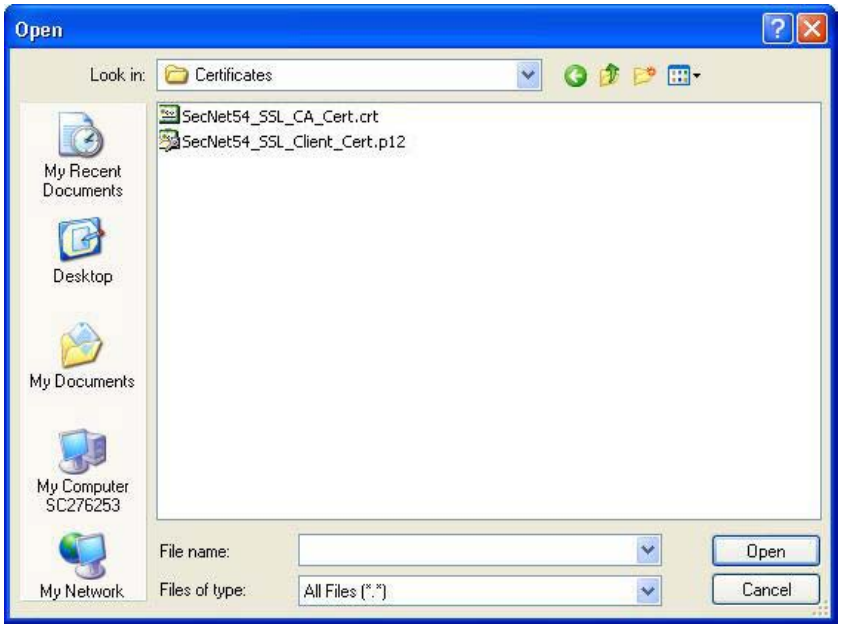
UNCLASSIFIED



UNCLASSIFIED

(U//FOUO) Selecting the **Browse...** button allows the User to locate the SecNet 54 SSL Client Certificate in the **Open** window.

UNCLASSIFIED//FOUO



UNCLASSFIED//FOUO

(U//FOUO) The “Look in” drop-down list box selection displays the drive containing the certificate. The selection of “All Files (*.*)” from the drop-down list box in the “File of type” displays all file types. Double-clicking the SecNet54_SSL_Client_Cert.p12 file displays the file path in the “File name” data field of the **Certificate Import Wizard** window. The wizard’s **Next >** button selection displays the **Password** page.

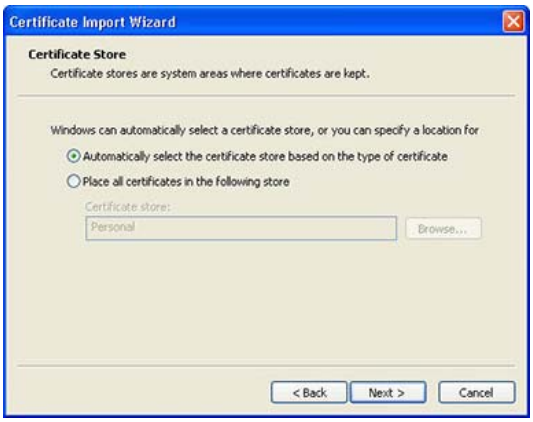
Appendix G (U) Importing SecNet 54 SSL Certificates into Web Browsers

UNCLASSIFIED

UNCLASSIFIED

(U//FOUO) The following password must be entered in lower case letters to access the private key: **secnet54**. Entering the password in the data entry field and selecting the **Next >** button display the **Certificate Store** page.

UNCLASSIFIED



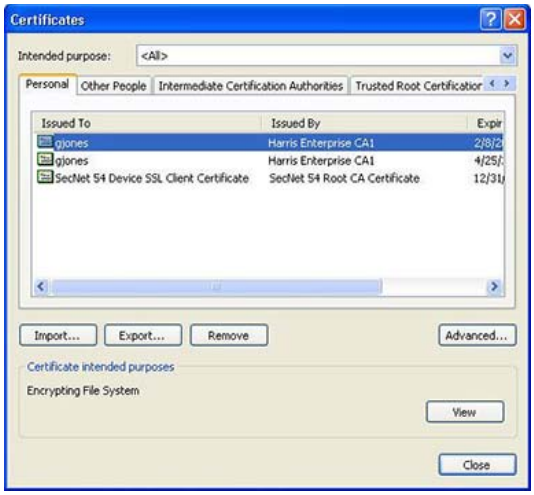
UNCLASSIFIED

(U) Selecting the radio button for “Automatically select the certificate store based on the type of certificate” specifies the criteria for the certificate store location. And, the **Next >** button selection displays a certificate import complete message within the wizard. The **Finish** button selection completes the import and displays the following pop-up message indicating a successful import:

The import was successful.

(U//FOUO) Verification of a successful import is accomplished by viewing the listing on the **Personal** tab within the **Certificates** window. The SecNet 54 Device SSL Client Certificate is listed in the “Issued To” column.

UNCLASSIFIED//FOUO



UNCLASSIFIED//FOUO

(U//FOUO) The SecNet 54 SSL Client Certificate is displayed when the certificate name and the **View** button are selection. The certificate indicates the intended purpose.

Appendix G (U) Importing SecNet 54 SSL Certificates into Web Browsers

UNCLASSIFIED//FOUO

UNCLASSIFEID//FOUO

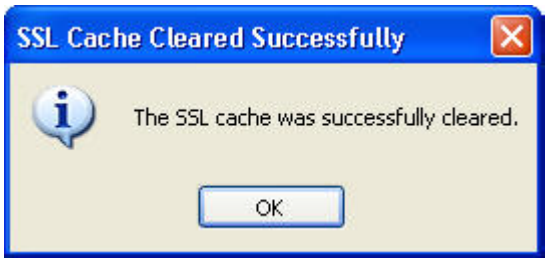
(U) The **OK** button selection closes the **Certificate** viewer, displaying the **Personal** tab in the **Certificates** window. The **Close** button selection removes the **Certificates** window and displays the **Internet Options** window.

UNCLASSIFIED

UNCLASSIFIED

(U) The **Internet Options** window provides a means to clear the SSL cache. Selecting the **Clear SSL State** button displays the following pop-up message:

UNCLASSIFIED



UNCLASSIFIED

(U//FOUO) The **OK** button selection from the pop-up window and then from the **Internet Option**s window removes both windows. It is recommended that the Web browser is closed and reopened before logging into a SecNet 54® device. Refer to Section G.5 for information on logging into the SecNet 54® device from a secure Web browser and acknowledging the SSL security alerts.

G.2.3 (U) Simultaneously Initiating the Import Process for the SecNet 54 SSL CA and Client Certificates

(U//FOUO) The SecNet 54 SSL CA Certificate must be installed before the SecNet 54 SSL Client Certificate. When the SSL CA Certificate is installed first, the browser will trust the SSL Client Certificate. If the SSL Client Certificate is not installed, the SecNet 54® device will not allow the connection to the Web browser. Although this section describes initiating the installation of both certificates together from one location, the CA Certificate is installed first (i.e., ".crt" file).

NOTE

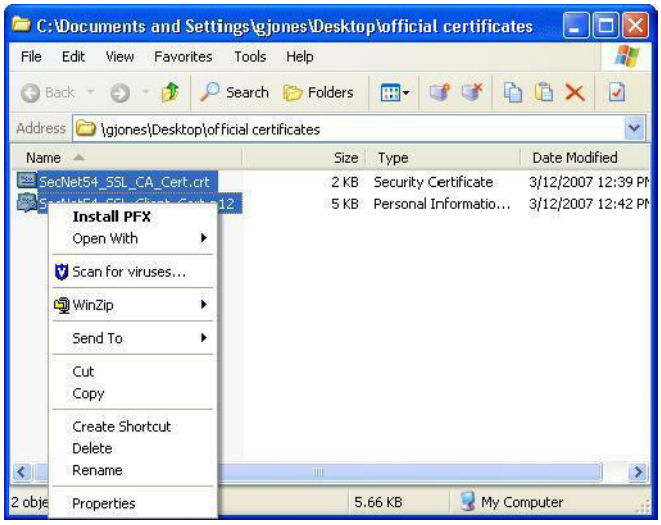
(U) The following certificates and associated data are examples. The actual certificate dates and associated data may differ when certificates are revised.

(U) When the following files are located, both are selected to begin the import process:

- (U//FOUO) SecNet_SSL_CA_Cert.crt
- (U//FOUO) SecNet_SSL_Client_Cert.p12

(U) Right-mouse clicking on the selected Client Certificate (i.e., ".p12" file) displays a pop-up menu.

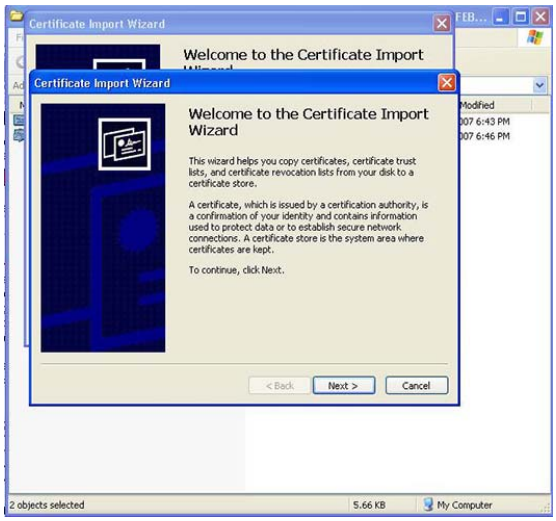
UNCLASSIFIED//FOUO



UNCLASSIFIED//FOUO

(U) When **Install PFX** is selected from the pop-up menu, two **Certificate Import Wizards** display with the wizard for the SSL CA Certificate window automatically displayed foremost. Note that if the pop-up menu does not display **Install PFX**, the right-mouse button selection occurred on the ".crt" file.

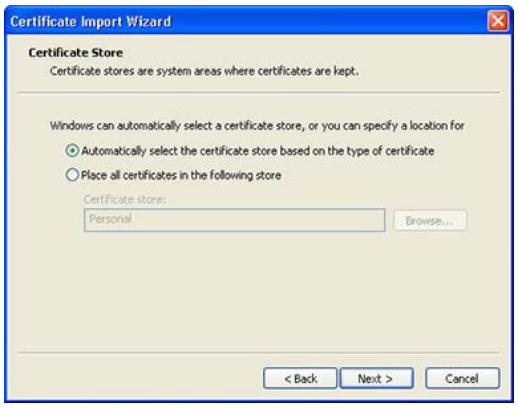
UNCLASSIFIED



UNCLASSIFIED

(U) Selecting the **Next>** button displays the **Certificate Store** page of the wizard with the default selection of “Automatically select the certificate store based on the type of certificate”. The selection specifies the criteria for the certificate store location.

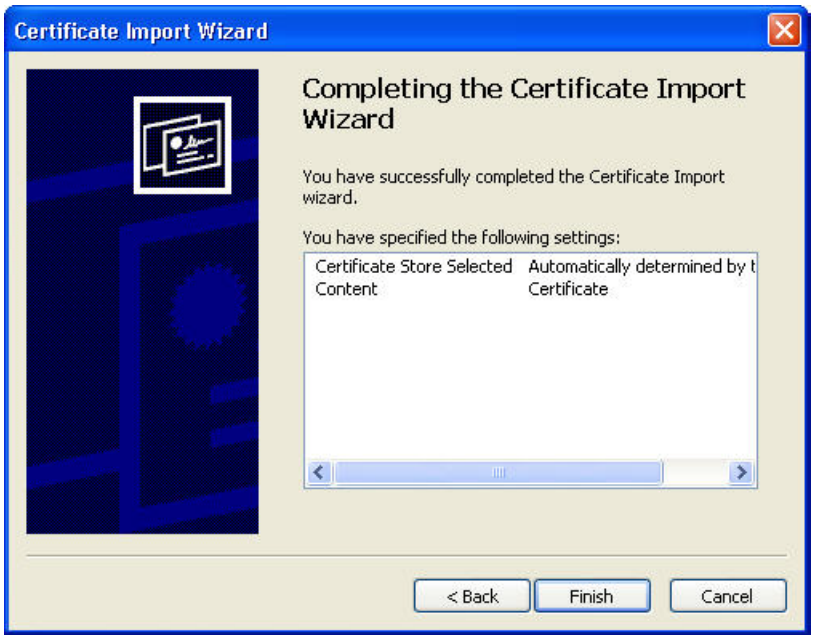
UNCLASSIFIED



UNCLASSIFED

(U) The **Next>** button selection displays the settings specified prior to completing the import process.

UNCLASSIFIED



UNCLASSIFIED

(U) The **Finish** button selection displays a **Security Warning** message with the name of the certificate indicated. Note that the file name can be verified as the appropriate CA Certificate to import.

UNCLASSIFIED//FOUO

UNCLASSIFIED//FOUO

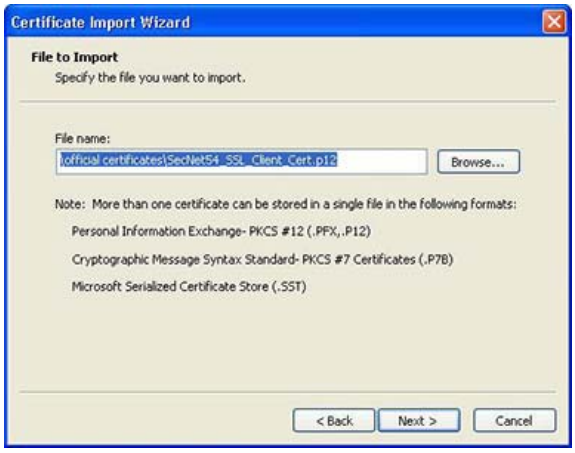
(U) The **Yes** button selection displays the following pop-up confirmation message indicating a successful import:

The import was successful.

(U) Selecting the **OK** button removes the confirmation message and displays the **Welcome to the Certificate Import Wizard** page for the SSL Client Certificate.

(U) Selecting the **Next>** button from the **Welcome to the Certificate Import Wizard** page displays the **File to Import** page with the SSL Client Certificate path in the "File Name" data entry field of the wizard. Note that the file location, name, and type can be verified as the appropriate file to import.

UNCLASSIFIED//FOUO



UNCLASSIFIED//FOUO

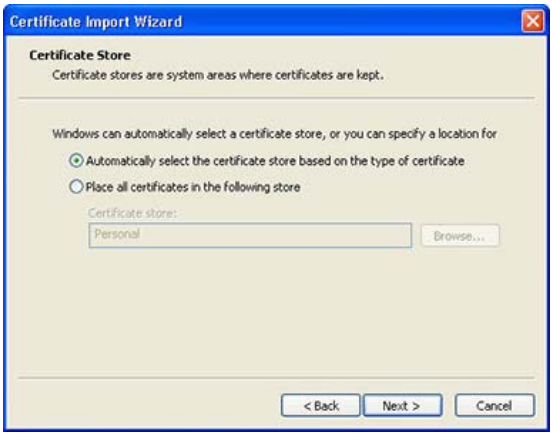
(U) The **Next>** button selection displays the **Password** page.

UNCLASSIED

UNCLASSIFIED

(U//FOUO) Entering the password of **secnet54** (in lowercase letters) provides access to the private key. After entering the password, selecting the **Next>** button displays the **Certificate Store** page with the default selection of “Automatically select the certificate store based on the type of certificate”. This selection specifies the criteria for the certificate store location.

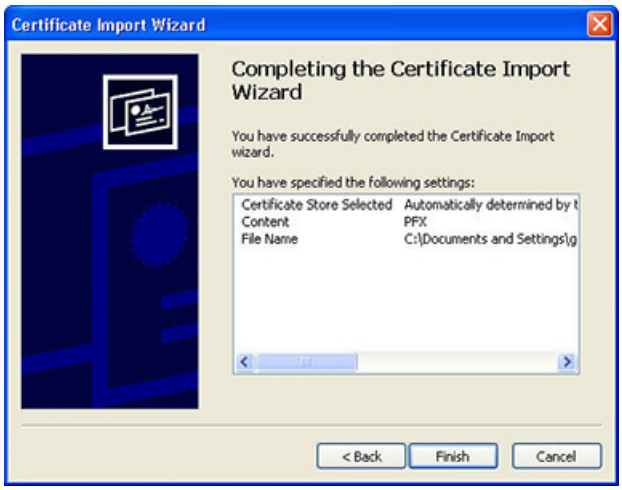
UNCLASSIFIED



UNCLASSIFIED

(U) The **Next>** button selection displays the settings specified prior to completing the import process.

UNCLASSIFIED



UNCLASSIFIED

(U) The **Finish** button selection completes the important process, removes the wizard, and displays the following pop-up confirmation message indicating a successful import:

The import was successful.

(U) Selecting the **OK** button removes the confirmation message.

(U) The IE Web browser provides a method to clear the SSL cache after certificates are installed. Opening the IE Web browser and selecting **Internet Options...** from the **Tools** submenu, as described in Section G.2.1, displays the **Internet Options** window. The **Content** tab selection displays three areas, including the **Certificates** area, from which to select the **Clear SSL State** button. When this button is selected, the SSL cache is cleared and a confirmation message is displayed.

Appendix G (U) Importing SecNet 54 SSL Certificates into Web Browsers

UNCLASSIFIED

UNCLASSIFIED

(U) It is recommended that the Web browser is closed and reopened before logging into the configuration Web pages.

G.3 (U) IMPORTING THE SECNET 54® SSL CERTIFICATES USING THE MOZILLA FIREFOX WEB BROWSERS

(U//FOUO) The SecNet 54 SSL CA Certificate must be installed before the SecNet 54 SSL Client Certificate. When the SSL CA Certificate is installed first, the browser will trust the SSL Client Certificate. If the SSL Client Certificate is not installed, the SecNet 54® device will not allow a connection to the Web browser.

NOTE

(U) The following certificates and associated data are examples. The actual certificate dates and associated data may differ when certificates are revised.

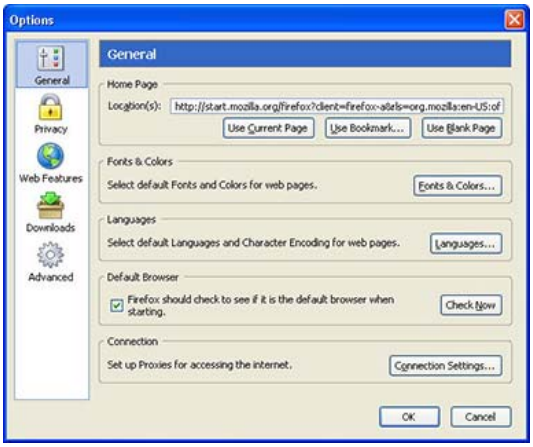
G.3.1 (U) Importing the SecNet 54 SSL CA Certificate Using the Mozilla Firefox Web Browser (Version 1.0.x)

(U//FOUO) The SecNet 54® SSL Certificate import process begins at the Mozilla Firefox (version 1.0.x) Web browser's main menu bar (refer to Section G.1). Selecting **Options** from the **Tools** submenu displays the **Options** window.

NOTE

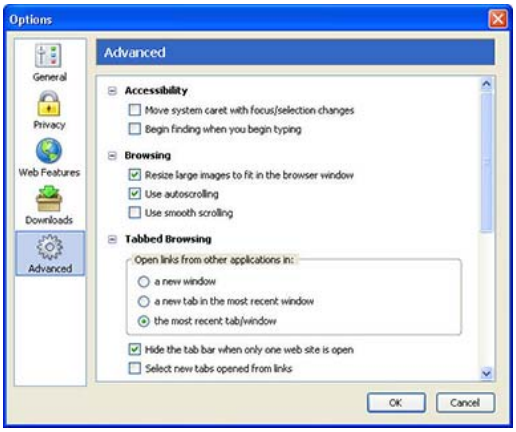
(U) On Linux computers, **Preferences** is selected from the **Edit** submenu to access the **Certificates** menu.

UNCLASSIFIED



UNCLASSIFIED

(U) The **Advanced** icon selection displays the **Advanced** options. The **Certificates** entry is displayed by scrolling down the list.

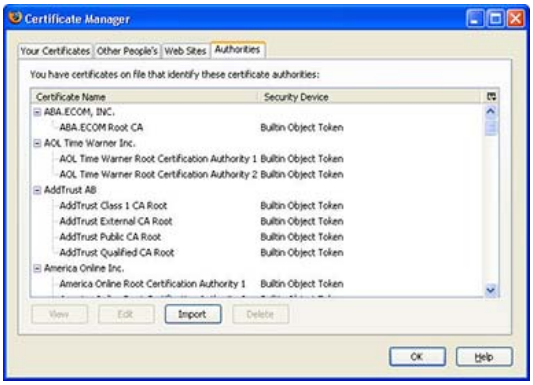


(U) Expanding the **Certificates** menu displays three areas, including the **Manage Certificates** area, as illustrated in the following figure.

(U//FOUO) The selection of the “Ask Every Time” radio button in the **Client Certificate Selection** area allows the User or Administrator to select the appropriate SecNet 54® SSL Certificate at each SecNet 54® configuration Web page login session. Failing to select this option may result in an error message and the SecNet 54® configuration Web pages not being accessible.

(U) The **Manage Certificates...** button selection displays the **Certificate Manager** window. The **Authorities** tab selection displays a listing of certificates that are currently loaded on the local computer.

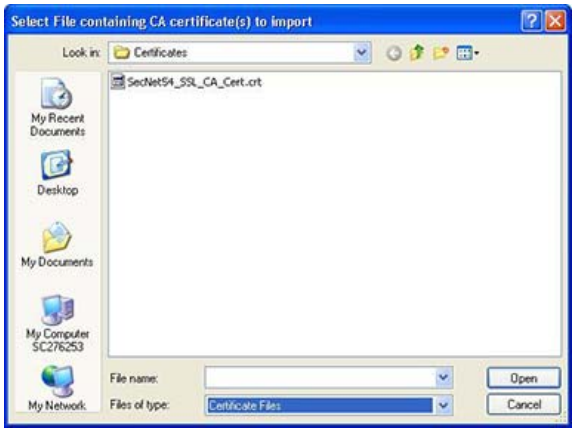
UNCLASSIFIED



UNCLASSIFIED

(U) The **Import** button selection displays the **Select File containing CA certificate(s) to import** window.

UNCLASSIFIED//FOUO



UNCLASSIFIED//FOUO

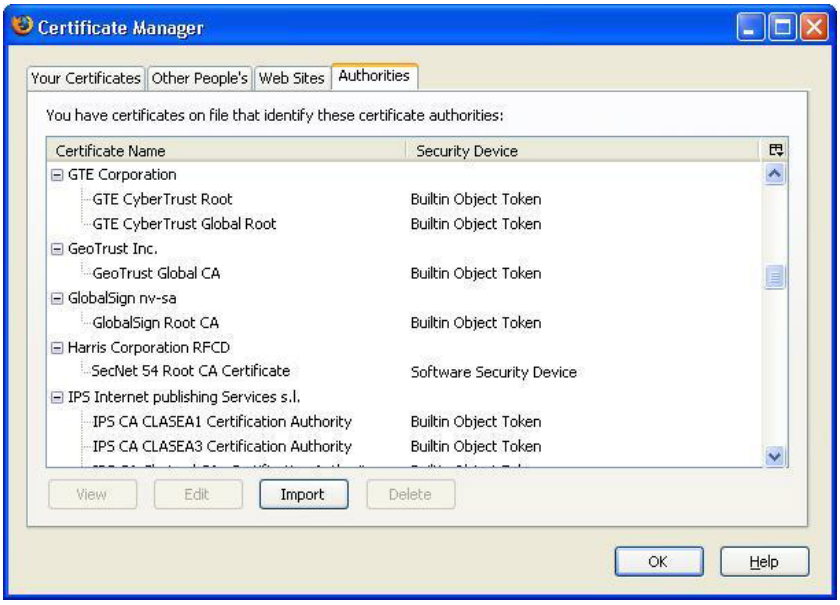
(U//FOUO) The “Look in” drop-down list box allows the User to browse the drive or desktop to locate the certificate. The selection of “All Files (*.*)” from the drop-down list box in the “Files of type” displays all file types located in a selected folder. Double-clicking the SecNet54_SSL_CA_Cert.crt file displays the **Downloading Certificate** window.

UNCLASSIFIED//FOUO

UNCLASSIFIED//FOUO

(U//FOUO) Selecting the “Trust this CA to identify Web sites” check box and the **OK** button redisplays the **Certificate Manager** window. The **Authorities** tab displays the SecNet 54 Root CA Certificate as published by Harris Corporation RFCD.

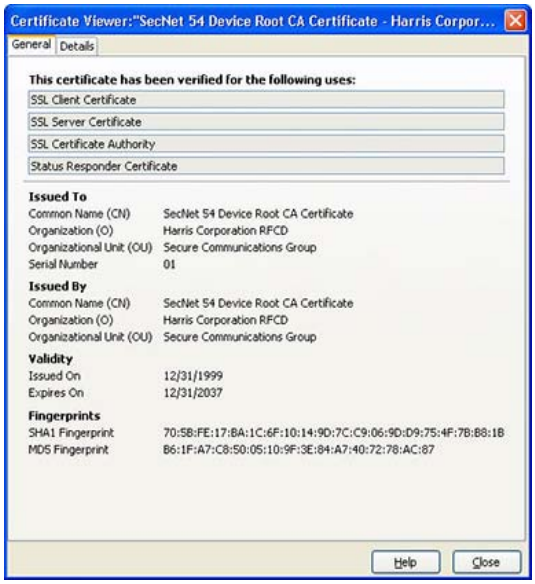
UNCLASSIFIED//FOUO



UNCLASSIFIED//FOUO

(U//FOUO) Selecting the SecNet 54 Root CA Certificate activates the **View** button. The **View** button selection displays the **Certificate Viewer** window, indicating that the certificate has been verified for the appropriate uses.

UNCLASSIFIED//FOUO



UNCLASSIFIED//FOUO

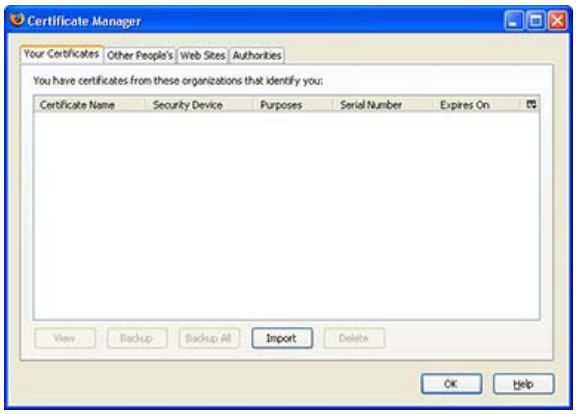
(U) The **Close** button selection removes the **Certificate Viewer** window, redisplaying the **Authorities** tab in the **Certificate Manager** window.

(U//FOUO) The client side certificate is also imported from the **Certificate Manager** window, as described in the following section, G.3.2. The SecNet 54 SSL Client Certificate must be installed to complete the two-way authentication.

G.3.2 (U) Importing the SecNet 54 SSL Client Certificate Using the Mozilla Firefox Web Browser (Version 1.0.x)

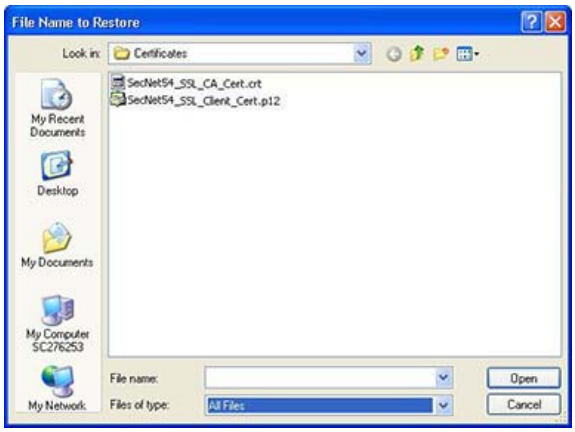
(U) Once the SSL CA Certificate has been imported, the SSL Client Certificate can be installed. Selecting the **Your Certificates** tab in the **Certificate Manager** window and the **Import** button displays the **File Name to Restore** window.

UNCLASSIFIED



UNCLASSIFIED

UNCLASSIFIED//FOUO



UNCLASSIFIED//FOUO

(U//FOUO) The “Look in” drop-down list box allows the User to browse the drive or desktop to locate the certificate. The selection of “All Files (*.*)” from the drop-down list box in the “Files of type” displays all file types located in a selected folder. Double-clicking the SecNet54_SSL_Client_Cert.p12 file displays the default **Change Master Password** window.

NOTE

(U) The **Change Master Password** window displays the first time the Client Certificate is loaded on the Mozilla browser. If a password has been previously defined, a different window displays, prompting the User for the master password for the software security device (refer to Section 3.2.2.2). However, if a New Password was not defined (i.e., “(not set)” saved) the first time the **Change Master Password** window displayed, this browser will not display the **Change Master Password** window or the **Prompt** window to enter a password.

UNCLASSIFIED

UNCLASSIFIED

(U//FOUO) The security device password is normally undefined. However, in this example the password is defined as **secnet54** in lowercase letters and is entered in both data entry fields. As the password is typed, the **OK** button becomes inactive and the “Password quality meter” is activated. Any errors while entering the passwords will cause the **OK** button to remain inactive until the data has been entered correctly. When the **OK** button is active and selected, a **Password Entry Dialog** box is displayed, prompting the User for the new password.

UNCLASSIFIED

UNCLASSIFIED

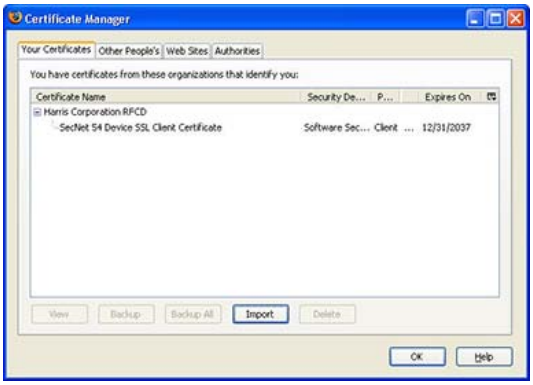
(U//FOUO) Entering the password of **secnet54** in lowercase letters and selecting the **OK** button remove the dialog and the following **Alert** window displays:

UNCLASSIFIED

UNCLASSIFIED

(U//FOUO) The **OK** button selection removes the **Alert** window and displays the **Your Certificates** page with the SecNet 54 Device SSL Client Certificate in the “Certificate Name” column.

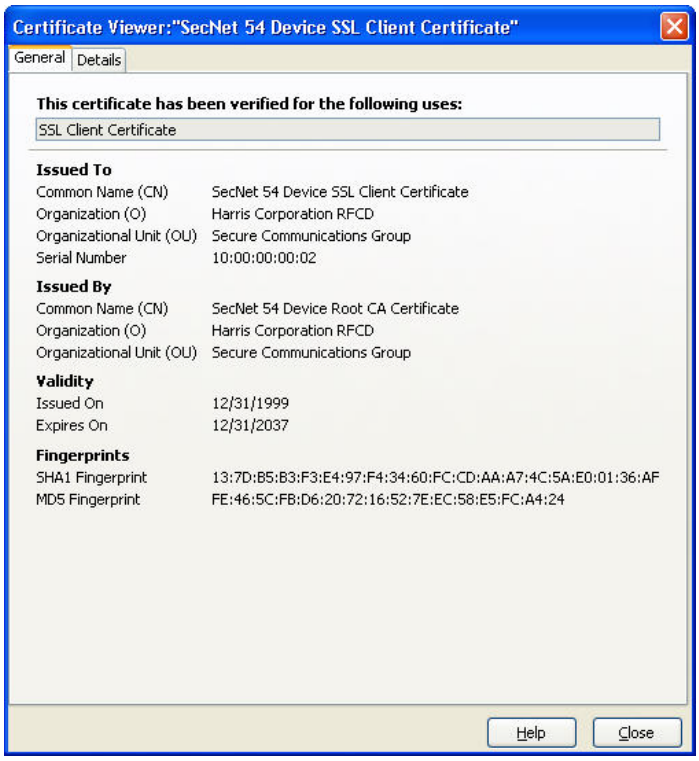
UNCLASSIFIED//FOUO



UNCLASSIFIED//FOUO

(U//FOUO) Selecting the SecNet 54 SSL Client Certificate activates the **View** button. The **View** button selection displays the **Certificate Viewer: "SecNet 54 Device SSL Client Certificate"** window, indicating that the certificate has been verified for use as an SSL Client Certificate.

UNCLASSIFIED//FOUO



UNCLASSIFIED//FOUO

(U) The **Close** button selection removes the viewer and redisplays the **Certificate Manager** window. The **OK** button selection from the **Certificate Manager** window and from the **Options** window removes both windows.

(U//FOUO) It is recommended that the Web browser is closed and reopened before logging into a SecNet 54® device. Refer to Section 3.2.2.3 for information about logging into the SecNet 54® device from the **DEVICE LOGIN** window.

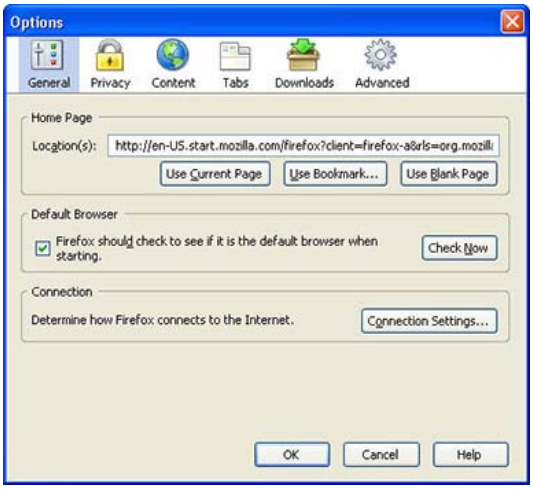
G.3.3 (U) Importing the SecNet 54 SSL CA Certificate Using the Mozilla Firefox Web Browser (Version 1.5.x)

(U//FOUO) The SecNet 54® SSL Certificate import process begins at the Mozilla Firefox (version 1.5.x) Web browser's main menu bar (refer to Section G.1). Selecting **Options** from the **Tools** submenu displays the **Options** window.

NOTE

(U) On Linux computers, **Preferences** is selected from the **Edit** submenu to access the **Certificates** menu.

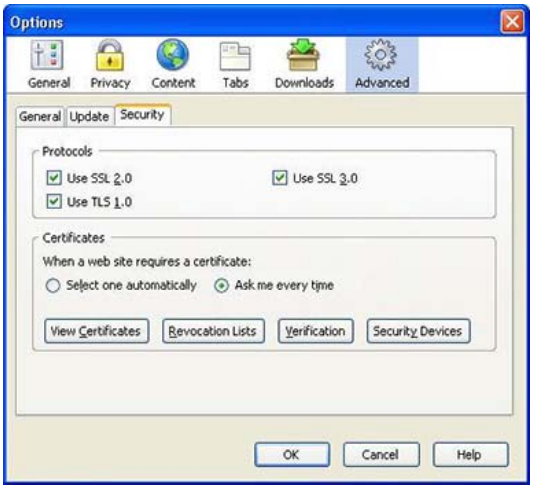
UNCLASSIFIED



UNCLASSIFIED

(U) The **Advanced** icon selection displays the **Advanced** options. The **Security** tab displays the options associated with the Certificates.

UNCLASSIFIED

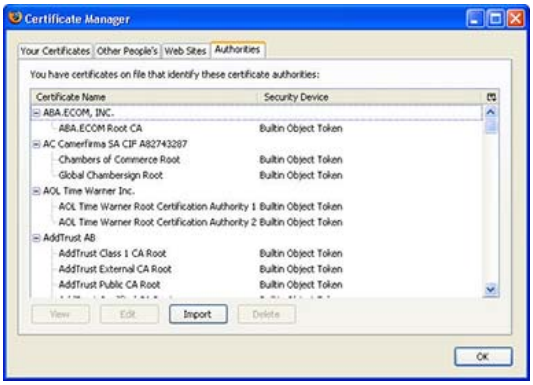


UNCLASSIFIED

(U//FOUO) The selection of the “Ask me every time” radio button in the **Certificates** area allows the User or Administrator to select the appropriate SecNet 54® SSL Certificate at each SecNet 54® configuration Web page login session. Failing to select this option may result in an error message and the SecNet 54® configuration Web pages not being accessible.

(U) The **View Certificates** button selection displays the **Certificate Manager** window. The **Authorities** tab selection displays a listing of certificates that are residing on the local computer.

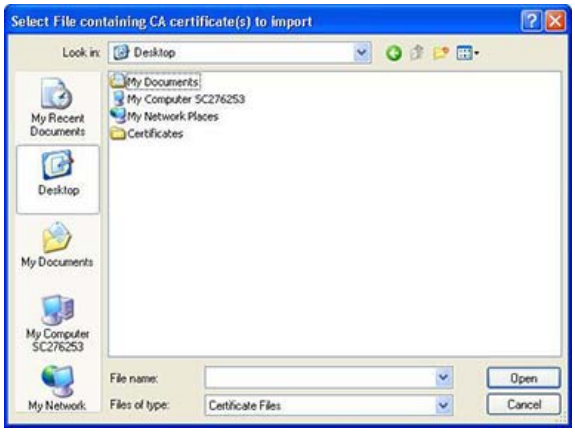
UNCLASSIFIED



UNCLASSIFIED

(U) The **Import** button selection displays the **Select File containing CA certificate(s) to import** window.

UNCLASSIFIED



UNCLASSIFIED

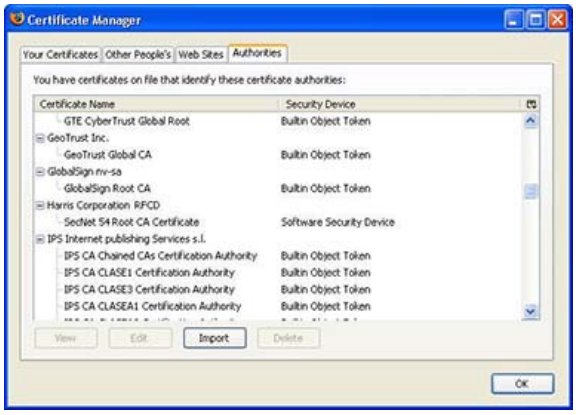
(U//FOUO) The “Look in” drop-down list box allows the User to browse the drive or desktop to locate the certificate. The selection of “All Files (*.*)” from the drop-down list box in the “Files of type” displays all file types located in a selected folder. Double-clicking the SecNet_54_SSL_CA_Cert.crt file displays the **Downloading Certificate** window.

UNCLASSIFIED//FOUO

UNCLASSIFIED//FOUO

(U//FOUO) Selecting the “Trust this CA to identify Web sites” check box and the **OK** button redisplays the **Certificate Manager** window. The **Authorities** tab displays the SecNet 54 Root CA Certificate as published by Harris Corporation RFCD.

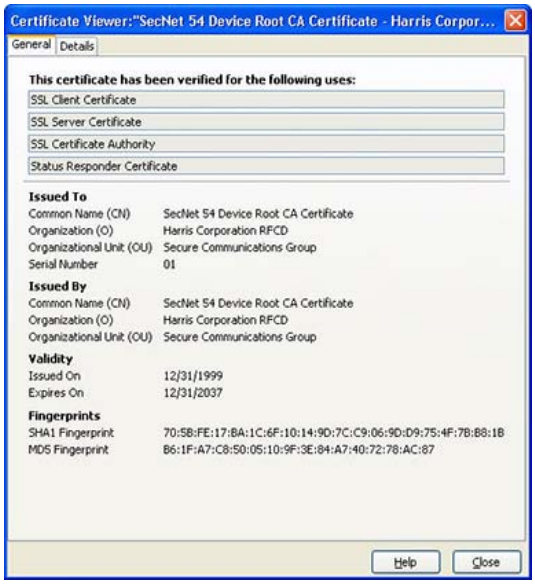
UNCLASSIFIED//FOUO



UNCLASSIFIED//FOUO

(U//FOUO) Selecting the SecNet 54 CA Certificate activates the **View** button. The **View** button selection displays the **Certificate Viewer** window, indicating that the certificate has been verified for the appropriate uses.

UNCLASSIFIED//FOUO



UNCLASSIFIED//FOUO

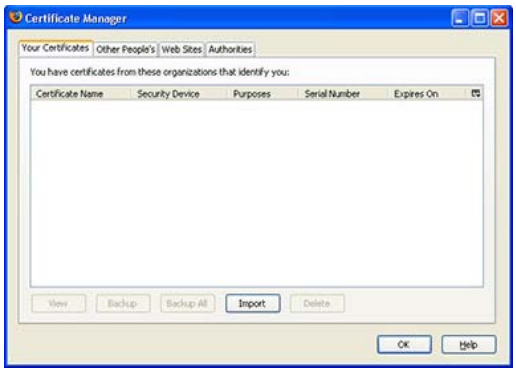
(U) The **Close** button selection closes the **Certificate Viewer** window, redisplaying the **Authorities** tab in the **Certificate Manager** window.

(U//FOUO) The client side certificate is also imported from the **Certificate Manager** window, as described in the following section, G.3.4. The SecNet 54 SSL Client Certificate must be installed to complete the two-way authentication.

G.3.4 (U) Importing the SecNet 54 SSL Client Certificate Using the Mozilla Firefox Web Browser (Version 1.5.x)

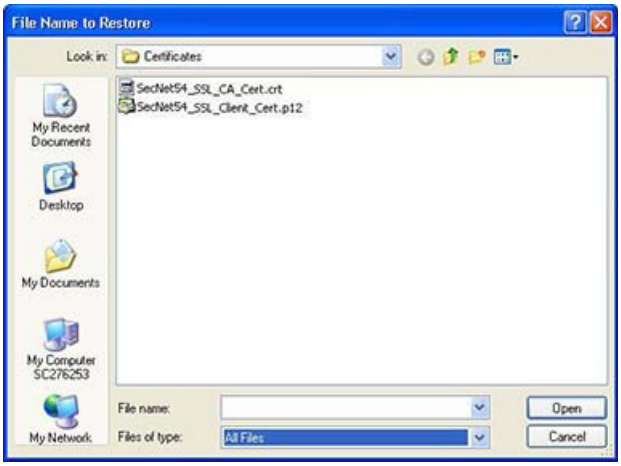
(U) Once the SSL CA Certificate has been imported, the SSL Client Certificate can be installed. Selecting the **Your Certificates** tab in the **Certificate Manager** window and then the **Import** button displays the **File Name to Restore** window.

UNCLASSIFIED



UNCLASSIFIED

UNCLASSIFIED//FOUO



UNCLASSIFIED//FOUO

(U//FOUO) The “Look in” drop-down list box allows the User to browse the drive or desktop to locate the certificate. The selection of “All Files (*.*)” from the drop-down list box in the “Files of type” displays all file types located in a selected folder. Double-clicking the SecNet54_SSL_Client_Cert.p12 file displays the **Prompt** window requesting the password. However, if a master password has not been defined (as described in Section G.3.2) when installing the SSL Client Certificate, this prompt will not appear.

UNCLASSIFIED

UNCLASSIFIED

NOTE

(U) If a Client Certificate has not been previously loaded into the Mozilla browser (any version), the default **Change Master Password** window is displayed. Refer to Section G.3.2.

(U//FOUO) In this example the password is **secnet54** in all lowercase letters. Entering the password and selecting the **OK** button display the **Password Entry Dialog** box.

UNCLASSIFIED

UNCLASSIFIED

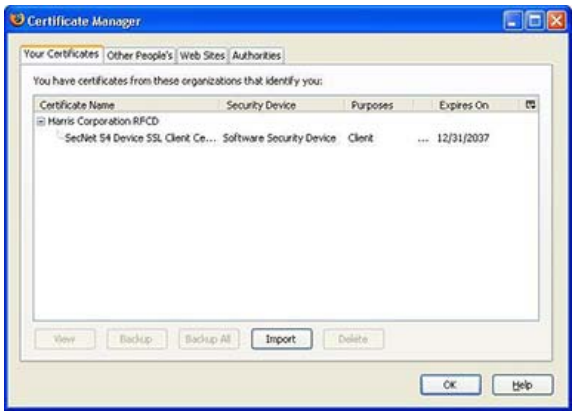
(U//FOUO) When the password is re-entered (i.e., **secnet54**) in the dialog box and the **OK** button is selected, an **Alert** window is displayed confirming the action.

UNCLASSIFIED

UNCLASSIFIED

(U) Selecting the **OK** button from the **Alert** window removes this window. The **Certificate Manager** window is displayed with the **Your Certificates** page visible and the Client Certificate installed.

UNCLASSIFIED//FOUO



UNCLASSIFIED//FOUO

(U//FOUO) Selecting the SecNet 54 SSL Client Certificate activates the **View** button. The **View** button selection displays the **Certificate Viewer: "SecNet 54 Device SSL Client Certificate"** window, indicating that the certificate has been verified for use as an SSL Client Certificate.

UNCLASSIFIED//FOUO

UNCLASSIFIED//FOUO

(U//FOUO) The **Close** button selection removes the certificate viewer and redisplays the **Your Certificates** page in the **Certificate Manager** window. Selecting the **OK** button from the **Certificate Manager** window and from the **Options** window closes both windows. It is recommended that the browser is closed and reopened before logging into a SecNet 54® device. Refer to Section 3.2.2.3 for information about logging into the SecNet 54® device from the **DEVICE LOGIN** window.

G.4 (U) IMPORTING THE SECNET 54® SSL CERTIFICATES USING THE NETSCAPE WEB BROWSER

(U//FOUO) The SecNet 54 SSL CA Certificate must be installed before the SecNet 54 SSL Client Certificate. When the SSL CA Certificate is installed first, the browser will trust the SSL Client Certificate. If the SSL Client Certificate is not installed, the SecNet 54® device will not allow a connection to the Web browser.

NOTE

(U) The following certificates and associated data are examples. The actual certificate dates and associated data may differ when certificates are revised.

G.4.1 (U) Importing the SecNet 54 SSL CA Certificate Using the Netscape Web Browser (Version 7.2)

(U//FOUO) The SecNet 54 SSL CA Certificate import process beings at the Netscape (version 7.2) Web browser's main menu bar (refer to Section G.1). Selecting **Preferences** from the **Edit** submenu displays the **Preferences** window.

UNCLASSIFIED

UNCLASSIFIED

(U) The privacy and security information is displayed from this window by expanding the Privacy & Security option under the **Category** listing, which is on the left side of the window.

UNCLASSIFIED

UNCLASSIFIED

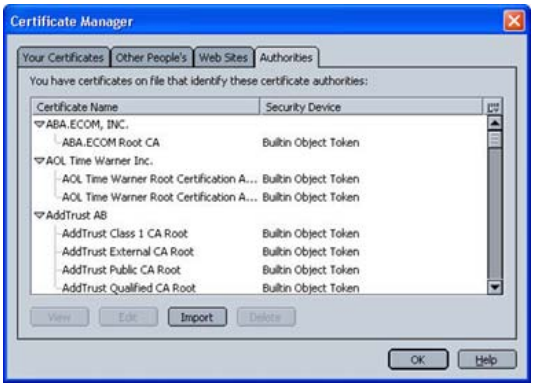
(U) The Certificates selection displays its associated options in the main window area.

UNCLASSIFIED

UNCLASSIFIED

(U) The **Manage Certificates...** button selection displays the **Certificate Manager** window. The **Authorities** tab selection displays the certificates residing on the local computer.

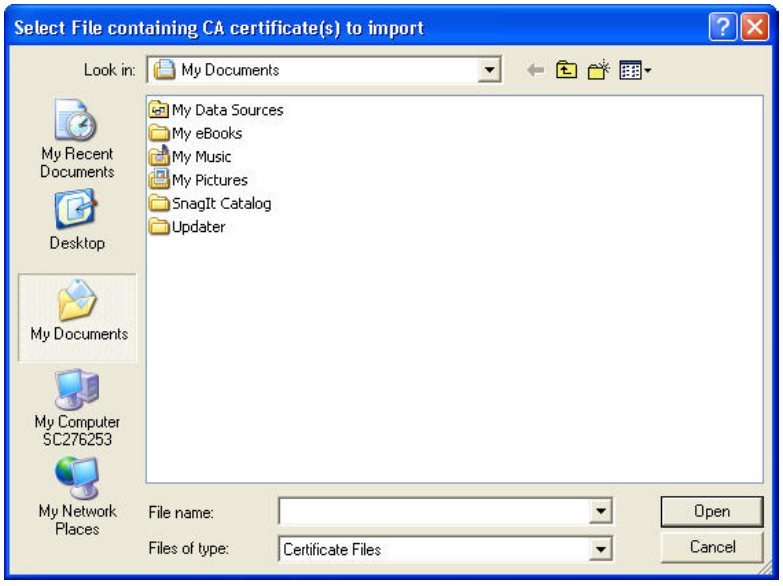
UNCLASSIFIED



UNCLASSIFIED

(U) The **Import** button selection displays the **Select File containing CA certificate(s) to import** window.

UNCLASSIFIED



UNCLASSIFIED

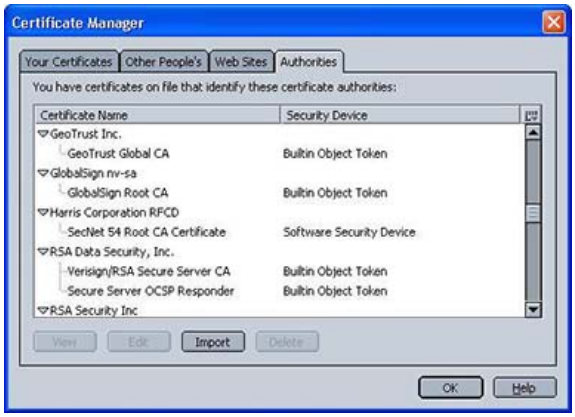
(U//FOUO) The “Look in” drop-down list box allows the User to browse the drive or desktop to locate the certificate. The selection of “All Files (*.*)” from the drop-down list box in the “Files of type” displays all file types located in a selected folder. Double-clicking the SecNet_54_Device_SSL_CA.crt file displays the **Downloading Certificate** window.

UNCLASSIFIED//FOUO

UNCLASSIFIED//FOUO

(U//FOUO) The selection of the check box associated with “Trust this CA to identify web sites.” and the **OK** button removes the window, redisplaying the **Certificate Manager** window. The **Authorities** tab selection displays the SecNet 54 Root CA under Harris Corporation RFCD.

UNCLASSIFIED//FOUO



UNCLASSIFIED//FOUO

(U//FOUO) Selecting the SecNet 54 Root CA Certificate activates the **View** button. The **View** button selection displays the **Certificate Viewer** window, indicating that the certificate has been verified for the appropriate uses.

UNCLASSIFIED//FOUO

UNCLASSIFIED//FOUO

(U) The **Close** button selection removes **Certificate Viewer** window and redisplays the **Downloading Certificates** window.

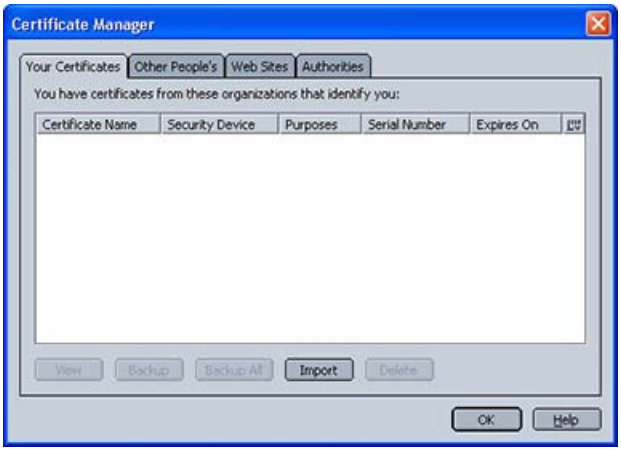
(U//FOUO) The following section, G.4.2, describes how to import the client side certificate from the **Certificate Manager** window. The SecNet 54 SSL Client Certificate must be installed to complete the two-way authentication.

G.4.2 (U) Importing the SecNet 54 SSL Client Certificate Using the Netscape Web Browser (Version 7.2)

(U) Once the SSL CA Certificate has been imported, the SSL Client Certificate can be installed. Selecting the **Your Certificates** tab in the **Certificate Manager** window and then the Import button displays the **File Name to Restore** window.

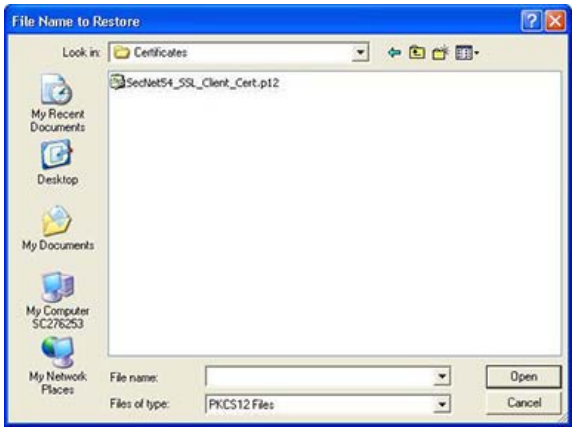
Appendix G (U) Importing SecNet 54 SSL Certificates into Web Browsers

UNCLASSIFIED



UNCLASSIFIED

UNCLASSIFIED//FOUO



UNCLASSIFIED//FOUO

(U//FOUO) The “Look in” drop-down list box allows the User to browse the drive or desktop to locate the certificate. The selection of “All Files (*.*)” from the drop-down list box in the “Files of type” displays all file types located in a selected folder. Double-clicking the SecNet54_SSL_Client_Cert.p12 file displays the **Change Master Password** window.

NOTE

(U) The **Change Master Password** window displays the first time the Client Certificate is loaded on the Netscape browser. If a password has been previously defined, a different window displays, prompting the User for the master password to the software security device. However, if a New Password was not defined (i.e., “(not set)” saved) the first time the **Change Master Password** window displayed, this browser will not display the **Change Master Password** window or the **Prompt** window to enter a password.

UNCLASSIFIED

UNCLASSIFIED

(U//FOUO) The security device password is normally undefined, However, in this example the password is defined as **secnet54** in lowercase letters and is entered in each data entry field. As the password is typed, the **OK** button becomes inactive and the “Password quality meter” is activated. Any errors while entering the passwords will cause the **OK** button to remain inactive until the data has been entered correctly. When the **OK** button is active and selected, a **Password Entry Dialog** box is displayed, prompting the User for the new password.

Appendix G (U) Importing SecNet 54 SSL Certificates into Web Browsers

UNCLASSIFIED

UNCLASSIFIED

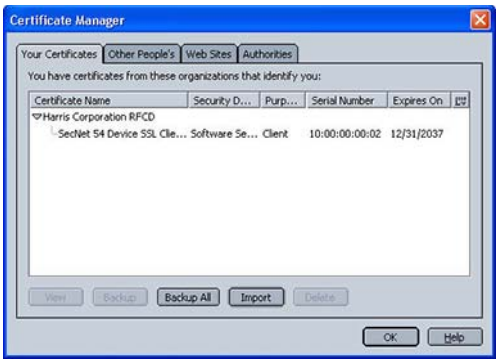
(U//FOUO) Entering the password of **secnet54** in lowercase letters and selecting the **OK** button remove the dialog and the following **Alert** window displays:

UNCLASSIFIED

UNCLASSIFIED

(U//FOUO) The **OK** button selection removes the **Alert** window, displaying the **Your Certificates** tab with the SecNet 54 Device SSL Client Certificate in the “Certificate Name” column.

UNCLASSIFIED//FOUO



UNCLASSIFIED//FOUO

(U//FOUO) Selecting the Client Certificate activates the **View** button. The **View** button selection displays the **Certificate Viewer: "SecNet 54 Device SSL Client Certificate"** window, indicating that the certificate has been verified for use as an SSL Client Certificate.

UNCLASSIFIED//FOUO

UNCLASSIFIED//FOUO

(U//FOUO) The **Close** button selection removes the viewer, redisplaying the **Certificate Manager** window. Selecting the **OK** button from the **Certificate Manager** window and then from the **Preferences** window removes both windows. It is recommended that the browser is closed and reopened before logging into a SecNet 54® device. Refer to Section G.5 for information on logging into the SecNet 54® device from a secure Web browser and acknowledging the SSL security alerts.

G.5 (U) ACKNOWLEDGING SSL SECURITY ALERTS DURING DEVICE LOGIN FROM A SECURE WEB BROWSER

NOTE

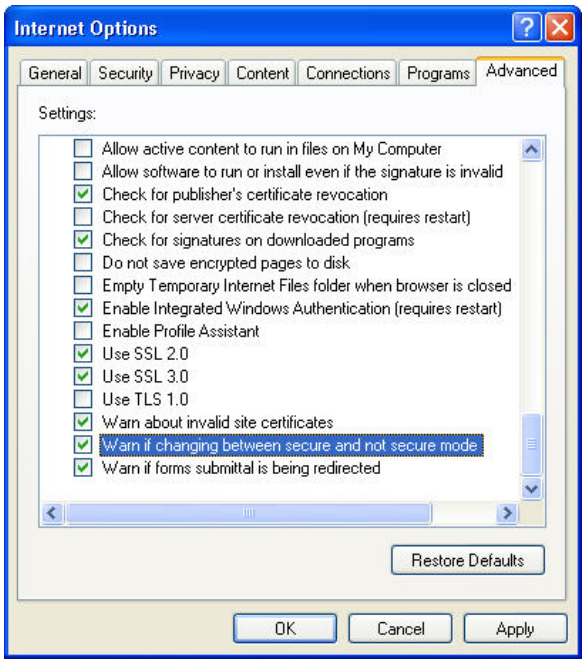
(U) The security alerts described in the following sections are not applicable when accessing the KIV-54 Web pages using the Mozilla Firefox Web browser.

G.5.1 (U) Acknowledging SSL Security Alerts from the IE Web Browser (Version 6.0)

(U//FOUO) When the KIV-54 Web pages are accessed from an IE Web browser and computer combination, an SSL **Security Alert** is displayed if the following conditions are met:

a. (U) The following checkbox is selected on the **Advanced** tab of the **Internet Options** window (refer to Section G.2.1): “Warn if changing between secure and not secure mode.”

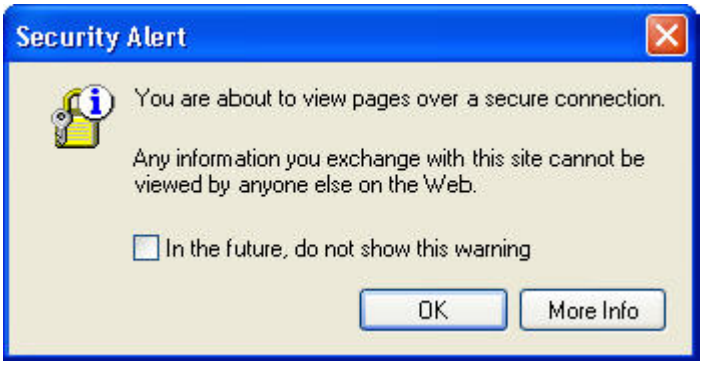
UNCLASSIFIED



UNCLASSIFIED

b. (U) The condition is met in Step "a" above and the following checkbox is not selected in the **Security Alert** window as illustrated below: "In the future, do not show this warning."

UNCLASSIFIED



UNCLASSIFIED

NOTE

TBD (U//FOUO) The Security Alert message (illustrated above) is not applicable when the IE Web browser is closed.

(U) Selecting the **OK** button displays another **Security Alert** window.

UNCLASSIFIED

UNCLASSIFIED

(U) From this **Security Alert** window the User verifies that there are green checkmarks applicable to "The security certificate is from a trusted certifying authority." and "The security certificate date is valid."

(U) The yellow warning symbol for the third option is allowed. Refer to the Frequently Asked Questions, Appendix B, for information about the first warning alert in the window.

NOTE

(U) Although the capability to import a certificate is provided from the **Security Alert** window, do not import a certificate using this method.

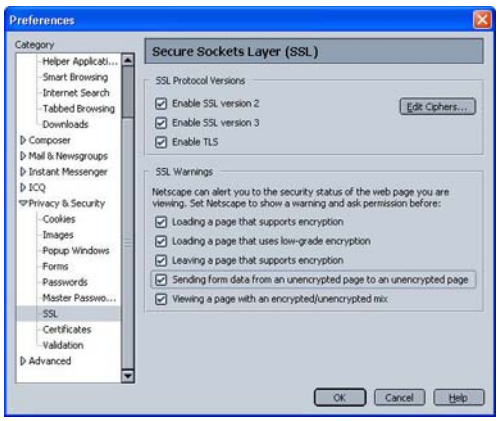
(U//FOUO) The **Yes** button selection allows the User to proceed to the **DEVICE LOGIN** Web page (refer to Section 3.2.2.3).

G.5.2 (U) Acknowledging SSL Security Alerts from the Netscape Web Browser (Version 7.0)

(U//FOUO) When the KIV-54 Web pages are accessed from a Netscape Web browser and computer combination, an SSL **Security Warning** is displayed if the following conditions are met:

a. (U) The following checkbox is selected on the "SSL Warning" area of the **Preferences** window (refer to Section G.4.1): "Sending form data from an unencrypted page to an encrypted page."

UNCLASSIFIED



UNCLASSIFIED

b. (U) The condition is met in Step "a" above and the following checkbox is selected in the **Security Warning** window as illustrated below: "Alert me whenever I am about to view an encrypted page."

UNCLASSIFIED

UNCLASSIFIED

NOTE

(U//FOUO) The Security Warning message (illustrated above) is not applicable when the Navigator Web browser is closed.

(U//FOUO) The **OK** button selection closes the window and displays the **DEVICE LOGIN** Web page (refer to Section 3.2.2.3).

(U) INDEX

(U) Index

RF Communications Division | 1680 University Ave | Rochester, NY USA 14610
Tel: 585-244-5830. Fax: 585-242-4755 **www.harris.com**